REPORT OF THE CHALLENGE 2000
SUBCOMMITTEE OF THE
FEDERAL AVIATION ADMINISTRATION
RESEARCH, ENGINEERING, AND DEVELOPMENT
ADVISORY COMMITTEE

FOR THE ADMINISTRATOR
OF THE FAA

THE HONORABLE DAVID R. HINSON

6 MARCH, 1996

REPORT OF THE CHALLENGE 2000 SUBCOMMITTEE OF THE F.A.A. RESEARCH, DEVELOPMENT, AND ADVISORY COMMITTE FOR THE ADMINISTRATOR AND THE AGENCY

BACKGROUND: On July 13th, 1995, the Administrator of the Federal Aviation Administration, Mr. David R. Hinson, announced a new initiative to re-examine the agency's fundamental approach to its' certification function and its future operation. This review was to consider more than the traditional certification process; it included the broader process of utilizing new technologies, additional administrative techniques, and other means of improving aviation safety. The review was also to include an examination of the impact of future technologies on this overall process of moving beyond the *enviable U.S. record of continually decreasing accident rates* to the means for **breaking through to a new, dramatic goal outlined by Administrator Hinson, of "near zero aircraft accidents"!**

The re-examination has focused mainly on the FAA's AVR organization. Nonetheless, the FAA's Executive Steering Committee included key policymakers from many organizations within the FAA. Additionally, the study effort utilized the Booz,Allen and Hamilton Corporation for studies of *comparative* safety critical activities as well as analyses of the FAA's existing certification structure. Finally, the examination of the impact of future technologies was tasked to the **FAA's Research, Engineering, and Development Advisory Committee**, who formed a special subcommittee for this task. This is the report of that special subcommittee.

Consistent with all activities of the FAA R.E.&D. Advisory Committee, this study was accomplished *strictly in accordance with the rules and procedures outlined in the U.S. Advisory Committee Act, and was an open and public process.* The special Challenge 2000 Subcommittee was led by Lt.General James A. Abrahamson, U.S. Air Force (retired), former Chairman of the FAA R.E.&D. Advisory Committee; and two leading members of the Advisory Committee: Mr. John Zugschwert, Vice President, Textron Corporation, and Mr. Bruce Landsberg, Executive Director of the Aircraft Owners and Pilots Association's Air Safety Foundation. **There were many major contributors and very special thanks go to each one who contributed enthusiastically and without compensation, these are listed at Appendix III. The FAA Federal**

Advisory Committee Official for this study effort was Ms. Nancy Lane. The FAA R.E.&D. Advisory Committee Federal Official is Dr. Andres Zellweger.

STRUCTURE OF THE REPORT

This report is structured in several sections. The Executive Summary contains an abbreviated discussion of the new technologies and their impact on the systems, the disciplines, and the functional approaches for improving air safety. It also contains a summary of the reports' principal recommendations.

The "New Technologies" section of the report is the output of Mr. Landsberg's subcommittee, which concentrated their efforts on an exposition of several existing or emerging, advanced technologies which will have a decided impact on the processes and administrative actions used by the FAA to enhance air safety. These vital FAA activities include certification, regulation, education and training, service bulletins, inspections, etc. They represent the full spectrum of FAA activities which influence and regulate the international aviation community on behalf of the safety and comfort of the citizens of the United States; as well as benefit people everywhere and assist in the development of safe and efficient air commerce and general aviation. The specific selection or group of advanced technologies discussed in this section is not intended to be exhaustive or complete. It is instead a selection of a group of technologies that will make a difference and will inexorably impact FAA safety enhancement and certification activities. *This impact could be to provide a unique opportunity to improve FAA processes or increase efficiency and effectiveness; or several technologies may represent trends which, if not adequately foreseen and prepared for, could undermine today's safety enhancement process.*

The "Systems and Functional Disciplines" section of the report is the output of Mr. Zugschwert's subcommittee. This team applied an alternate working approach that recognized that all major aviation activities are made up of interacting systems. For example, the design and development of a new transport aircraft involves structural design that starts with complex structural models of the new design, implements the design with tools—models—and analyses to ensure the aircraft will be structurally safe, and will operate over a lifetime in many different environments (most probably even in ways that are not foreseen at the time of the initial design). Therefore, the requirements development process, strength of materials calculations, stress equations, aerodynamic stress and lifetime predictive modeling, automated manufacturing techniques, and many other design support activities are all individual, multifaceted, complex “systems” in their own right.

All of the above systems must be theoretically and practically correct, must maintain integrity, must be operated and controlled by human beings as well as computers, and finally they must interact in a way that does not invalidate the limitations of the individual systems. Further, aircraft operations involve many conglomerations of systems, such as the aircraft electrical systems, engine systems, support systems, etc. As these systems interact, they must also be controlled. This can only be accomplished with the aid of special management activities such as---flight safety, human factors, quality control and other disciplines.

Therefore, Mr. Zugschwert’s subcommittee has approached the problem of enhancing air safety, by examining the implications of new technologies for “systems,” and for the “disciplines” of flight safety, human factors, etc. A clear area of emphasis is the issue of the use of Commercial Off-The-Shelf (COTS) technology, particularly COTS software and related COTS computer systems.

Appendix I is a review of COTS issues by Dr. George Allen of TRW, Corp. Appendix II is a listing of key individuals who have contributed to this study effort or to the report itself. Volume II is a compilation of the papers that were submitted by individuals or by organizations to the subcommittee. These are included, so that the FAA or the public may have the full benefit of many thoughtful inputs that have been incorporated or summarized in the report.

ACKNOWLEDGMENT

The participants and subcommittee members who have participated in this study effort wish to thank the FAA for the privilege of allowing us to express a wide variety of opinions, suggestions, and to provide in-depth expositions on what technologies and disciplines may make a real difference in air safety for the future, as well as significantly affect the way in which the FAA conducts one of its most vital missions.

We were all impressed by the scope and importance of Administrator Hinson’s initiative, by the constructive way the Challenge 2000 Executive Committee and the people of the FAA approached the study, and by the response of many individual volunteers and companies who

contributed! We also deeply appreciated the opportunity to work with the Booz, Allen & Hamilton consultant team. *Finally, as always for FAA R.E.&D. Advisory Committee efforts, we wish to especially acknowledge the important supervision of our volunteer efforts by the FAA Advisory Committee designated Federal Officials and by the FAA legal staff.*

TABLE OF CONTENTS

EXECUTIVE SUMMARY OF THE REPORT

The Federal Aviation Administration (FAA), world Civil Aviation Authorities, the military services, and many other government and civil institutions as well as companies around the globe are facing the combined challenges of adopting to rapidly changing technologies with decreasing levels of human and capital resources. For the aviation industry this problem is exacerbated by an unprecedented growth in air commerce! None-the-less, the Federal Aviation Administration, working with the aviation industry, the airlines as well as general aviation aircraft owners, operators, and pilots---all have worked successfully to bring the U.S. aircraft accident rate to a dramatic and historic minimum level, but this will not be enough. ***Even if today's accident rates, were sustained or slightly improved, the growth in air travel is projected to be so significant that the absolute number of accidents that would be so high and so frequent that people everywhere would react in horror! The prospect of this potential problem and the difficulty of finding ways to avoid it underscore the importance of Administrator Hinson's challenge to the FAA, the aviation industry and all of us to find ways to continue to lower future aircraft accident rates to near zero!***

A vital arm of the FAA for enhancing safety is the Office of Regulation and Certification (AVR), led by Mr. Anthony Broderick and manned by an excellent, dedicated work force of approximately 5,000 people, operating in well over 100 locations in the United States, with extended activities around the world. The people of AVR deserve great credit and the continued appreciation of Americans and people everywhere, who today can confidently look forward to a safe and secure flight on U.S. (and on most international) airlines as well as in business and general aviation aircraft. *The dedication of the people of AVR, along with their procedures and regulatory structure, working with the aviation industry, airlines and general aviation infrastructure, have helped in a very significant way to provide safe and robust air commerce and air travel that is fundamental to every aspect of our modern way of life!*

Nonetheless, AVR and the FAA will be faced with the certainty of vastly increased scope of responsibilities and relatively reduced human and financial resources with which to tackle an exploding mission! Thus, Administrator Hinson's "Challenge 2000" study to explore alternatives for AVR and their FAA supporting activities is a vital and timely management initiative for the future of the FAA and for air commerce.

This report is the result of the FAA's Administrator's request to the FAA's R.E.&D. Advisory Committee to examine the impact of future technologies on AVR and on the FAA's process of certification, regulation, as well as other approaches to enhancing flight safety. This study is a separate effort from the Booz, Allen, and Hamilton contracted study, but it is an integral part of the overall Challenge 2000 review. It should be examined in conjunction with the Booz, Allen, and Hamilton study and the FAA's internal review of future AVR operations.

TECHNOLOGIES THAT WILL IMPACT AVR AND THE FAA: In the future, many technologies will have a profound effect on the aviation industry, thereby impacting the ways that AVR and the FAA conduct their regulatory and safety enhancing functions. In addition to those aviation related technologies, others will provide either a direct opportunity or a threat to the existing methods and procedures of AVR and the FAA. Thus, both categories of technology need to be properly anticipated. The following selection of technologies, include both of the above categories. However, the following list of technologies "that will make a difference" is not intended to be a complete or even a *prioritized* list of technologies. Forecasting technology is always difficult and more characterized by mistakes and surprises rather than by prescient knowledge or instinct.

But first, there are two vital, technology-based, *over-riding* themes that must be articulated and thoughtfully addressed by any regulatory or "technology controlling" agency as it looks to the future:

AN AGGRESSIVE, CONSISTENT AND ENLIGHTENED SCIENTIFIC APPROACH TO CERTIFICATION AND THE INTRODUCTION OF NEW TECHNOLOGIES IS VITAL TO BOTH THE ECONOMIC FUTURE OF U.S. AVIATION AND THE

ABILITY OF THE FAA TO MEET THE CHALLENGE OF SIGNIFICANTLY LOWERING FUTURE ACCIDENT RATES TO NEAR-ZERO LEVELS!

- AVR has been effective in supporting both FAA and aviation goals with aggressive and effective certification activities. This record is clearly apparent in the certification of GPS overlay approaches, in the recent record of certifying the Boeing 777, and other efforts certifying general aviation aircraft and key components.

- It is also imperative that AVR maintain a responsible certification program that does not prematurely advance technologies or designs that are not safe. This "balance" puts great pressure on FAA personnel, and must be executed well and with consistency.

- As technology advances in the future, a less than optimal approach by AVR could slow the introduction of vital advances for U.S. technology leadership, could tend to retard the general pace of technology in aeronautics, or could delay the introduction of new safety-related equipment and procedures. For example, the U.S. FAA is the certification agency of choice today for U.S. industry (and for some international certifications as well)...**if industry leaders perceive that we are not willing to maintain technology leadership for the future, they will take products and innovation elsewhere and the U.S. will quickly fall behind the advancing front of aeronautical technology.**

- Thus, it is fundamental that AVR and its FAA and industry supporting elements be supported with resources as well as the advanced systems to maintain and improve the agency's "forward looking" and scientifically enlightened approach to advanced technology.

AVR SHOULD BE SUPPORTED WITH NEW, HIGHLY TECHNICAL HUMAN RESOURCES; ADDITIONAL TRAINING FOR AVR'S EXPERIENCED AND VERY VALUABLE WORKFORCE; AND NEW SYSTEMS AND SUPPORT TO DEAL

WITH RAPIDLY ADVANCING AERONAUTICAL TECHNOLOGIES--ESPECIALLY IN THE AREAS OF INFORMATION AND TELECOMMUNICATIONS TECHNOLOGIES AND COMPUTER HARDWARE AND SOFTWARE SYSTEMS.

The following list of technologies offers a “ranging selection” of well-founded “impacting technologies”...with arguments (*primarily contained in the full report*,) of why and how these technologies need to be carefully considered as AVR and the FAA restructure organizations, policies, procedures, trained personnel, and install advanced systems for the future.

1. The single, most profound, and influential family of technological advances for our modern era is in the field of **Advanced Information Systems.** This includes the advances in information processing theory, telecommunications, advanced computer hardware and most of all the explosion in software. As discussed in the main body of the report, this field is characterized today by accelerating advances in each of the above areas; and these synergistically combine to produce changes that are dramatically altering every aspect of our society and each field of technology. Advanced Information System technologies will provide amazing opportunities and impact every area of the aviation industry. They will also provide procedural and human interaction capabilities that must be captured by AVR and by the FAA in every phase of their mission.

2. The FAA and CAA’s around the world are capturing the new navigation paradigms associated with **navigation satellites (GNSS) and planning for the safety and capacity improvements on the horizon with advanced Communications, Navigation and Surveillance systems (CNS), and the potential of “Free Flight”** concepts for improved Air Traffic Management (ATM). The FAA and AVR should be commended for their global leadership in this important area and they will be challenged as these concepts and systems are implemented on a global basis.

3. A technology that already has and in the future will, more importantly impact, aircraft structures and components is the field

of **composites.** *Again the FAA and NASA as well as the military services and commercial industry must all take credit for the solid scientific and engineering work that has already been accomplished to responsibly develop this revolution in aircraft construction.* However, additional engineering, certification, and safety work must be accomplished before the promise of this technology is fully realized. *Everyone must understand that this revolution is as far-reaching today, as the transformation from wood, wire, and canvas to metal aircraft was in the nineteen thirties.*

4. Today's **Advanced Simulation technologies** also impact the process of setting requirements for aviation and ATM, the aircraft design process, the manufacturing process, the support process, training, and many more. This advanced simulation capability is not restricted to the highly capable flight simulators that have become so important to flight crew training. It also includes scientific simulation, rapid prototyping, partial task simulations, comparisons between equipment aging characteristics and original tested performance, etc. Simulation technology is rapidly becoming the method of choice to both understand "human factor" problems (the single most important cause of accidents in every phase of aviation) and the best method of minimizing random and inconsistent human behavior. Thus, full utilization of all types of simulation technology will be basic to AVR, the FAA, and the industry as we pursue "near zero accident rate" goals in the future.

5. A technology application that has been discussed, but not adequately considered is the rapid advance in reliability, performance, and broad operating range of **commercial electronic equipment.** For example, laptop computers are often utilized in flight test programs, general aviation pilots often utilize "hand-held" GPS receivers (sometimes illegally), and upcoming candidate technologies for aviation could soon include flat panel displays and virtual reality glasses.

The categories of commercial electronic equipment of concern are those developed for ground applications, not airborne usage. The promise and performance of many of these items of electronic equipment are so significant that AVR should carefully consider both its policies and approach for approving flight applications of commercial electronic equipment. This review should start well before before proposals for certification of these types of components not designed for airborne use begin streaming into the agency.

6. A special category of advanced electronic equipment is the rapidly developing field of **advanced sensors and synthetic vision**. This field is developing rapidly and applications, such as "heads up" displays for automobiles and boats will provide lower technology and price levels for aircraft systems. AVR has already helped advance the efficiency of airline operations through early certification of selective equipment. This technology deserves the encouragement of "regulatory pull" as investors and manufacturers consider broader applications for general aviation.

7. A different application for advanced sensors is the development of **new sensors and techniques for non-destructive testing of aircraft structures and components.** Some examples of promising NDI technologies are "holographic imaging of ultra-sound sensors"; electron beam and neutron inspection cameras and others. While these techniques may, in the future, offer quick and effective means for large scale structural verification....they will also be a scientific challenge for operators and for certification.

The examination of new technologies and their impact on vital Systems and Disciplines in use for "Quality Management", for "Human Factor" research and training, etc. are outlined in Section II of this report. Also included are appendices that provide a much more detailed treatment of the difficult subject of enhancing safety and certification of "Commercial Off-The-Shelf software technology systems"...COTS software. *These topics along with the discussion of the above technologies that can make significant differences for the aviation industry---and for the processes in use within AVR and the FAA, all lead to the following recommendations:*

R-1: AVR should build on appropriate aviation industry initiatives to develop the capacity to more effectively utilize electronic data interchange technologies with electronic data warehousing, and the subsequent capability to selectively call up and use digital technical data for analysis, for reliability and engineering support for certification, and to assist in aircraft lifetime accident prevention activities.

R-2: AVR should make it a priority to upgrade the information systems and computer skills of its personnel and gain access to experts with advanced knowledge of standards, electronic commerce, and advanced information processing systems.

R-3: To accelerate the next phase of certification of ATM procedures for GNSS, CNS, and Free-Flight...AVR should increase the use of statistical data sampling and simulation for flight procedure certification--- which can enable reduced flight check programs. A well structured effort could incentivize early aircraft equipage and save resources for the FAA.

R-4: AVR should enhance its already effective program of gathering data and enhancing certification for composite structures by working closely with other key agencies and industry to develop a detailed and accelerated, overall inter-agency "Master Plan" for verification and flight certification of composite technologies. This plan should include intensive data warehousing from all operating entities that fly aircraft with composite components.

R-5: AVR should investigate the issues associated with upgrading commercial electronic equipment such as computers, displays, automotive HUD's, etc. It must be recognized that these items were developed for non-safety critical use on the ground, but the benefits for aviation use of these rapidly advancing items of technology warrant a review and the potential development of guidelines for commercial avionics upgrades.

R-6: AVR should continue to emphasize technology advances such as new types of advanced sensors for reliable manufacturing, for providing intimate data on the state of equipment and aircraft, and for new techniques of extending pilot capabilities.

R-7: The FAA should refine its capability to identify new technology areas that could have an important role in reducing future accidents (i.e. many of the means discussed in this report).

AVR can assist by examining its regulatory process with the goal of creating a “compelling” process to help industry create “irresistible technical and business” incentives to develop and certify products to enhance safety in those identified areas.

R-8: AVR (through the FAA R&D organization) should expand full simulation as well as “rapid prototyping” human factor studies targeted at areas identified with “high accident potential” and associated with equipment and procedural certification. This effort should be worked jointly with NASA and the DOD.

R-9: AVR (through R&D) should explore new simulation support software in conjunction with other civilian and government agencies, vitally interested in human factor research. They should help mature the best tools to deal with safety, certification, and to support prevention efforts for “near zero accidents”.

R-10: AVR--in combination with FAA R&D efforts, with NASA, DOD, industry, and academia--should expand the use of interviews and opinion polls throughout the aviation industry to create a better means of projecting the potential for future accidents. This data should be combined with simulation and selectively used through data warehousing.

R-11: FAA should utilize every opportunity to develop and use “computer based training” for its own people, and encourage its use in aviation. AVR should find ways to use CBT to disseminate critical human factor lessons to help avoid accidents.

R-12: AVR should increase the use of Integrated Product Team (IPT) management of certification and safety enhancement functions.

R-13: AVR should hire more National Resource Specialists to increase in-house technical expertise to deal with the rapid acceleration of aeronautical technology.

R-14: Recommendations from the COTS/NDI report (at Appendix I):

A. The FAA should conduct an in-depth analysis of processes within the FAA which are affected by COTS/NDI technologies. This analysis should address the following:

1. Selection and engineering use guidelines.

2. Ideas for measuring and estimating the complexity of systems.

3. Develop a tailored life cycle model that addresses COTS / NDI components used in safety critical systems.

4. Develop a process to conduct preliminary risk assessments of systems that plan to use COTS / NDI.

5. Identify new methods to test and validate safety-critical systems which are not dependent on source code analysis.

6. Investigate ways to reduce the cost and time required to establish high confidence in a system.

7. Investigate ways to reduce cost and time required to re-establish high confidence in a system after a change is made.

8. Investigate ways to deal with interdependent properties and disciplines.

9. Explore domain specific architecture techniques to facilitate development and certification.

10. Develop new ideas to “fire-wall” functionality of COTS / NDI components within domain specific architectures.

11. Develop guidelines for use of NDI components acquired from domain-specific and general “re-use libraries”.

12. Demonstrate the cost-effectiveness of the above techniques.

13. The FAA analyze internal roles and responsibilities to include the following:

14. Investigate ways to involve critical functional elements of the FAA earlier in the system specification phase.

15. Assess modifications of the certification process and responsibilities to employ a “quick analysis” capability.

16. Identify ways to communicate to assurance and certification people.

17. Become a Beta test site for COTS products that are candidates for use in FAA domain specific architectures.

18. Promote software technology and process improvement techniques based on established best practice techniques.

19. Explore ways to expand current tracking of anomalies of COTS/NDI products by keeping statistics on product use throughout the computing industry.

Additionally, the full report that follows includes a significant number of issues and discussions that all bear on the exploitation of rapidly advancing technologies to improve AVR procedures and operations and to enhance flight safety. Several of these discussions include such issues as the following: the impact of the "demise of Military Specifications" on civil configuration management and certification; the impact of "electronic commerce" on the structure and enduring industrial relationships within the aerospace industry; the use of Integrated Product Teams, as well as other key issues.

Finally, the Challenge 2000 Subcommittee of the FAA R.E.&D. Advisory Committee has been pleased to participate in Administrator Hinson's important management initiative. We commend the FAA, AVR and the Executive Committee for their counsel and cooperation throughout the study. We also must commend the people of AVR for the exceptional service they perform for air commerce and for every aircraft passenger or crewmember.

SECTION I—NEW TECHNOLOGIES

"THAT WILL MAKE A DIFFERENCE"!

The combined forces of rapid technological change, decreased resources, and massive buildup in air commerce and air travel mean that the aviation industry as well as the FAA must both take "fresh looks" at the way things are done. The following group of advanced technologies will both challenge the FAA's certification process, and can also serve as technology opportunities to enhance safety, efficiency, and effectiveness. These technologies were not selected for study, merely because they exist or could exist. The following criteria were utilized to ensure relevancy and help select these technologies from an unbounded group of emerging technical capabilities*: a. Does it solve a pressing problem in aviation? b. Does the technology have appropriate reliability? c. Does the technology provide good human factors design possibilities? d. How will this technology interact with other systems?*

ADVANCED INFORMATION SYSTEMS CAPABILITIES

The revolution in advanced information technologies is changing the face of global business and society itself. The U.S. and many other countries often describe this revolution as the "Information Highway". The initial embodiment of this force for change is the Internet—an exploding network of networks that provides amazing new levels of connectivity for both industry and private individuals. Related to these astounding internet capabilities, telecommunications companies are making massive investments in fibre-optics trunk and even neighborhood connecting lines. When these are considered along with the low-cost ISDN lines for industry as well as industrial Local and Wide Area Networking---the result is high-speed, high bandwidth, highly flexible networking which also can provide reliable, redundant, secure switching with transmission for both analog and digital signals. These advanced telecommunication capabilities, coupled with advances in computing are opening previously unimagined industrial and personal applications.

Computing advances start with a dynamic software revolution built around the following kinds of fundamental capabilities:

advanced relational and object data-bases; imaging data storage and retrieval advances; smart retrieval tools; linking middleware; data warehousing; advanced and more and more user friendly “Graphical User Interfaces”; interactive, multi-media capabilities; object oriented programming tools and methodologies; and many more!

Although the usual process of developing and producing the above, mostly commercial software products does not ensure widespread and equivalent values of reliability, predictability, or even consistent long-term support capabilities, the potential for lower cost, partially re-usable, and accelerated product maturity is so high that the advantages of these COTS software programs are clear, and it is inevitable that many will be used in every aspect of the aviation industry as well as for Air Traffic Management (ATM).

Finally, the multiplier effect of the synergy between advanced telecommunications and software capabilities is even further enhanced by the following kinds of advances in computers and computer-support hardware: advanced “standard” integrated circuit chips with breakthroughs in reliability, low-cost, wide-environmental performance limits, and supportability; new standard “RISC” chips and astounding memory device advances; loosely coupled—massively parallel computer architectures, improved color screens, virtual reality glasses as well as flat-panel display advances; lithium-polymer batteries for portable devices; and many more.

A particularly promising combined technology advance is the concept of network computing, with its promise of very low costs, and extremely compact computing devices able to utilize remote software programming and storage in such a way that overall device performance will be substantially increased while promising cost reductions of factors of ten or more!

These combined advances are not breakthroughs in any one instance, rather, the **synergy and steady advance associated with all of the above technology areas are creating rapidly succeeding vistas of rich new capabilities**. As they are combined and specific new applications are developed, we have a critical *family of* *“technologies that imply major differences, threats, and opportunities for the FAA’s safety enhancement and regulatory processes:*

In the next few years, many aviation-related industries will enhance and complete their ongoing information system upgrades and new---enhanced, automated “data warehouses” will be in place, supporting most aspects of their businesses. For example, Boeing Corporation is well into a fundamental business process re-engineering effort, that is being combined with massive hardware and software upgrades to create a whole new work and information paradigm for the company.

McDonnell-Douglas has initiated a similar initiative, but with a different dimension—theirs is also an “electronic commerce” initiative being implemented on a project basis that will interconnect joint projects with British Aerospace. A similar “business process re-engineering” initiative is underway at Northrop Corporation, with their initial effort started at the Commercial Aircraft Division (whose main product line is the aft fuselage of the Boeing 747). Many other similar efforts are underway with most of the large and small companies who are at all levels of subcontracting in the civil and military aerospace industry.

Each of these above efforts is a vital initiative, aimed at taking advantage of the progress in information technologies (mentioned above) to establish whole new ways for humans to communicate and work together. Usually these are conceived architected, financed, and implemented at the individual corporation level. The implications of this individual company focus are the following: (a) the job becomes implementable....because it’s scope is both manageable and can be funded within a single company—that’s the good news! (b) although there are many standards bodies working on the problem of global electronic commerce (tying individual companies’ automation efforts together by means of international and national standards)....there is still only modest progress. This means that the individual systems being implemented in different companies often have very different components and may not be compatible within the context of larger “cross-company” enterprises---that’s the bad news!

In other words, we can look forward in a few years to a future with mature automation and information systems in place in many corporations....all with profound impacts on the capability and efficiency of those corporate enterprises. Hopefully, standards and system interface technology will keep pace with these “many islands of information systems”. But if not, we may have to “strap together” these advanced systems with interface systems. which in the past have often been both expensive and inefficient.

All of the competitive reasons that are forcing companies around the world to make huge investments in these advanced systems and revised processes, apply to government....to the FAA.....and to AVR! This information system trend is an inevitable one and it spawns a very vital question: *Since AVR’s functions are more human and regulation or judgementally centered than automation centered, how far should AVR go in trying to take advantage of these industrial initiatives?*

The subcommittee notes that from the very early days of the Air Traffic organization within the FAA (and especially since the early eighties), it has been a matter of faith that “increased automation would be a fundamental requirement for improved ATM operations”. We believe that AVR has already undertaken important automated management improvement efforts, which have demonstrated the value of automation systems to FAA regulatory activities. In particular, we commend the development of ASAP (the Aviation Safety Accident Prevention System, which provides information from the operators’ “Service Difficulty Reporting” database for FAA analysis); the CAAMS (the Continued Air-worthiness Assessment Methodology System, which assists AVR in focusing their resources around critical accident causal factors); the SPAS (the Safety Performance Analysis System which helps FAA air carrier inspectors focus on especially sensitive airline potential problem areas); and other advanced information system monitoring and automation initiatives! Finally, the subcommittee firmly believes that the proper implementation of additional advanced information systems could be as important to AVR's mission in the future as it is to Air Traffic for ATM.

R-1: AVR SHOULD BUILD ON APPROPRIATE AVIATION INDUSTRY INITIATIVES TO DEVELOP THE CAPACITY TO MORE EFFECTIVELY UTILIZE ELECTRONIC DATA INTERCHANGE TECHNOLOGIES; WITH ELECTRONIC DATA WAREHOUSING; AND THE CAPABILITY TO SELECTIVELY CALL UP AND USE DIGITAL TECHNICAL DATA--- FOR ANALYSIS, FOR RELIABILITY AND ENGINEERING SUPPORT, FOR CERTIFICATION, AND TO ASSIST IN AIRCRAFT LIFETIME ACCIDENT PREVENTION ACTIVITIES.

This recommendation is also consistent with themes of the 1995 Safety Data Collection and Use Workshop as well as other workshops reported in the draft Aviation Safety Plan for 1996--their recommendations follow:

- Both the government and industry need to improve their safety analysis capability;
- The availability of safety-related data must be increased for both FAA and industry; and (see next page)
- Actions should be taken to encourage development and use of airline partnership joint safety programs that include the sharing of information from airline crews and maintenance personnel.

[Additional pertinent recommendations are in the emerging technologies area of the draft report of the Safety Data and Collections workshop #4.]

- Initiate a process to use industry-collected data to identify systemic problems related to aircraft design and manufacture.....(and)
- Begin using industry-collected data to identify systemic problems in aircraft fleets, aviation personnel, and maintenance.

ISSUES FOR CONSIDERATION ASSOCIATED WITH INCREASED DATA WAREHOUSING FOR A BROADER BENEFIT TO THE FAA:

Implementation: Recommendation One is *not intended to suggest to AVR or more broadly to the FAA that they embark on the development of a complex data warehouse capability and then to impose burdensome requirements on industry to submit data for central storage and use.* Rather it is intended to point out the potential benefits of being able to selectively utilize the revolutionary telecommunications and data warehousing trends that are sweeping industry! If reasonable means can be found to accomplish this, it should not impose a major resource or systems requirement on AVR. However, some additional computer, software and human resources would probably be required. A method of exploring this problem would be to convene an RTCA Task Force or a periodic Industry Workshop to evaluate the issues and beneficial means of implementation. This forum should consider the following issues as well.

Reasonable Standardization: Airframe and engine manufacturers, component suppliers, etc. all have the requirement to maintain production and quality records today. In the past and in many cases still, these records are paper records that are mostly kept in broadly distributed locations at the original manufacturer's location. There is minimal standardization associated with those paper records. Airlines and private aircraft owners and operators also have the requirement to maintain more standard forms on the periodic maintenance of aircraft in accordance with approved procedures. As discussed above, the important steps already underway to digitize, automate, and improve the storage, retrieval, and use of production and ongoing maintenance information are most often centered around systems individualized to each company---this points to the importance of standards.

Unfortunately, there are few real standards being implemented across multiple enterprises, standards that would allow suppliers throughout the aviation industry to provide consistent, compatible data. This information could be best utilized in formats that would allow electronic exchange of information, automated quality monitoring and call- up speedy recall and transmittal to a central authority for emergencies (or accident investigation). etc.

However, data sharing will only be possible if adequate safeguards are included to protect proprietary information and to protect manufacturers and operators from unreasonable intrusion and unfair litigation!

While the possibilities and benefits of higher levels of standardization and computability are easy to imagine and describe; the challenge of developing flexible standards and architectures that can adopt to future growth and at the same time serve and protect broad and diverse parts of industry as well as the government's regulatory and accident prevention functions on an economical basis, is truly daunting. None-the-less, *this process will not get easier with time*. Companies are proceeding now with their individually optimized solutions and delay will only result in greater sunk investment and greater resistance to change to conform to broader standards. Thus, one issue for continued industry discussion with AVR is the ongoing process of separate enterprise data warehousing and the benefits that could well develop through an appropriate level of standardization to enhance information sharing, while protecting company's sensitive information.

Types of Information: The rapid advances in imaging technology make it clear that the variety of data and information that merits retention can be dramatically improved in future digital data warehouses. As discussed above, the formats of most of the required data storage today are paper records of inspections [often merely an inspector's stamp signifying that the inspection was conducted and met acceptable performance requirements]. Sometimes numbers are included, such as circuit parameters, accuracy of instruments in a test range, engine thrust at specific RPM, etc.; and/or comments [i.e. "corrosion was noted on the starboard flap hinge"].

As discussed in more detail below, new nondestructive test techniques and new approaches for obtaining diagnostic information are being developed every day. Many of these are graphic and provide much better information than a subjective comment or measurement of a single numerical value. i.e. infra-red pictures of the flame patterns and hot spots up the tailpipe of a jet engine [to detect areas of high stress or non-linear aerodynamic and heating effects], photographs of die-penetrant corrosion tests or a value map of eddy-current parameters in highly susceptible corrosion areas, and many others. Storage, call-up, and automated classification and comparison of some of these advanced image-format test results is possible and will be highly beneficial in a broader regime of automated, digital information warehousing.

AVR, with appropriate R&D elements of the FAA, with NASA, and with the military services or other interested organizations (such as the Air Transport Association), should find ways to encourage the twin objectives of finding new tests to diagnose trends and avoid failures as well as ensuring that software techniques are available and cost effective for storage, selective-cross-enterprise access and call-up, and for controlled and distributed use of information from these advanced, imaging tests.

Digital Warehousing of “Reusable Engineering”: At least one major airframe company is automating the testing, and support information required for initial certification of a new aircraft design. Additionally, several airframe and engine companies have implicitly utilized the concept of “re-useable engineering” in similar families of aircraft. Component manufacturers have for decades implicitly done the same thing as they move through subsequent versions and improvements of a piece of equipment. The means of ensuring that fundamental certification limitations or assumptions have not been violated in this process have mostly been implicit and judgmental. The possibilities for automating both of these aspects of design, certification, and related maintenance support is also an opportunity to enhance the discipline and safety associated with this process. In that vein, *automation features can be used to make a judgmental process quite visible.* Through that visibility comes the opportunity to ensure integrity of the design assumptions and explicit attention to questionable areas. These advantages accrue even in the face of changes in design or FAA changes in certification personnel, responsibilities, etc....and these benefits may be possible to include in an FAA and industry initiative for enhanced data warehousing.

The Demise of Military Specifications: A topic that is closely related to the "implicit assumptions and processes" discussed in the paragraph above, is the **implicit lower limit of certification of any component**. For example, the certification of a "black box" [i.e. an electronic component like a flight control computer] includes extensive testing of the overall box functions, it includes configuration control of circuit boards, integrated circuit chips, etc. However, rarely is there a separate certification of the specific chips, wiring harnesses, or other circuit elements. **At these lower levels, purchase specifications become a major tool for design and process control**. However, the amount of attention then paid to the quality history, historical environmental performance, stress levels and usage histories, etc. at those lower levels of design can sometimes then be uneven, judgmental, or implicit—when compared to the level of control inherent in the basic certification process.

In the past, there was excellent reason to have high confidence in the purchase specification system, because it often used actual or was derived from the "military-specification system." And there existed an extensive military control system for the design and manufacture of the "mil-spec" class of components. As "mil-spec" parts are being abandoned in favor of commercial components....this becomes a "bad news—good news" story. The bad news is that the military control system is first loosened, and will eventually become obsolete and abandoned. Therefore a source of design and manufacturing quality will be lost.

The good news is that many commercial components are now driven by the market place to supply and document levels of reliability, breadth of environmental performance, production quality control, testing....many of the elements of control that were previously only applied to military and aviation components! The problem for the future of FAA certification and specification...*especially for that implicit bottom end of the design*, is as follows: What is the level of design and manufacturing quality control, repeatability, and configuration management across a variety of bottom-end components, etc. and how will this be documented in the initial certification process and surveiled over the lifetime of the component?

In an important sense, this problem of implicit versus explicit definition of the bottom end of the certification process and the transition to reliance on commercial specifications or even just the excellence of the civil commercial marketplace is directly analogous to the “re-useable engineering” issue discussed above. Fortunately, increased use of and automated data warehousing can and should address these issues.

Incident Reporting: Data warehousing can be integrated with AVR’s other initiatives to gather information on and analyze both manufacturing and operational incidents as an automated alerting mechanism to help prevent accidents and equipment failures. Since the majority of these incidents are usually the result of human failures, rather than automated processes or procedural errors....the most important data for these automated alerting systems must be improved means of isolating and reporting human failures, warehousing them for comparison, and establishing trend data. Solid and complete incident reporting has been repeatedly proven to be the best predictor of accident potential....and *the key to accident prevention is to ensure that there are reliable and timely methods of getting this incident information to key decision makers at several levels. This is primarily an industrial responsibility, but AVR has both a responsibility and a stake in improving the integrity of the process....automation and data warehousing can help.*

Airworthiness Certification Fraud: Recent newspaper headlines have trumpeted several cases of airline parts fraud in several nations. The fact that these practices were uncovered at all, points to another FAA success story. These cases are often the joint initiatives of the FAA and the U.S. Department of Justice or sometimes our FAA working with international Civil Aeronautics Authorities. The criminal essence of many of these fraudulent sales of aircraft parts is that the airworthiness certificates are faked or sometimes non-existent. *A properly constructed interactive and distributed data warehousing initiative, serving both the FAA and* *industry, could simply and easily provide additional integrity information and make "aircraft parts fraud" a much more difficult enterprise!*

Electronic Commerce: The era of the "Information Highway" is also the era of "Electronic Commerce" (EC). The same synergistic advances in telecommunications, advanced software, and amazing—low cost computation hardware are changing the methodology and the vertical and horizontal structures of many industries. Earlier industrial enterprises were often reasonably stable; with well defined roles and relationships between customers and contractors, and between prime contractors and many levels of suppliers.

The design, development, production, support, and operations of an aircraft is a major enterprise involving many different companies, services, operations, and capabilities; as well as many levels of suppliers. Stability in the aviation industry has been created and controlled by procedures, contracts, specifications, personal communications between key individuals, control by customers and government agencies. Importantly, all aspects of corporate relationships in the aviation industry were relatively enduring. *If this relative stability is compared to the practice in industries who are rapidly moving into EC, we see the future in a highly competitive and dynamic marketplace.* We can foresee contracts being let electronically (often for smaller lot sizes or designed to fit into small openings in an ongoing 24 hour per day production schedule). Quality information is and will also be electronically transmitted. Even negotiations will most often occur via computer communications.

The by-words of the era of electronic commerce are speed, flexibility, competition, quality, and performance. In the earlier aviation marketplace, certification was the critical, enabling step for entry and a continued role in the marketplace. International trade was then enabled by government-to-government cooperative agreements and permission to conduct first hand inspections.

In the era of EC, for some aviation industry suppliers, it will become nearly impossible to continue certification and carefully surveil every airframe or electronic component supplier, the silicon foundries, software houses, fastener manufacturers, etc. Thus, the era of EC will inevitably challenge FAA approaches to certification, reliability, and safety as they are applied today. It will put new stresses on already stretched FAA human resources and budgets. International "offset" and other global enterprise forces will additionally stress today's successful practices.

Nations or regions of the world are focusing on standards for data exchange, product description, electronic contracting, quality control, etc. Many companies and some countries see a competitive advantage in having their standard adopted on a global basis [witness the ongoing international debate on the U.N sponsored global EDIFACT standard for EC versus the older and established ANSI X-12 standard, broadly implemented in the United States]. *Even in the highly cooperative, international aviation industry, ignoring standards development and delaying implementation of modern data warehousing and EC capabilities can be a fatal mistake.*

Continued FAA international leadership as well as successful transition to data warehousing, electronic commerce, advanced simulations and all the other complex, information-rich applications of the near future will require new emphasis and expertise in computer science. *This comment carries no negative connotation for the men and women of today's FAA. The requirement to dramatically upgrade skills for the information age is universal, and a need of nearly every institution, company, and government agency*. Thus, the FAA should make it a priority to upgrade computer skills at all levels and within all organizations of the agency, including AVR. This should include hiring new computer scientists, software engineers, etc. It should include gaining the expertise and access to key standards activities in the United States and abroad. It is equally important that the FAA's present dedicated, and experienced workforce should be given special courses, have access to symposia, and be provided "on-the-job" opportunities to gain special experience with advanced information and data centered computer systems!

R-2: AVR SHOULD MAKE IT A PRIORITY TO UPGRADE THE INFORMATION AND COMPUTER SKILLS OF ITS PERSONNEL

AND GAIN ACCESS TO EXPERTS WITH ADVANCED KNOWLEDGE OF STANDARDS, ELECTRONIC COMMERCE, AND ADVANCED INFORMATION PROCESSING SYSTEMS.

THE IMPACT OF GNSS AND CNS ATM

A second grouping of advanced technologies that will significantly affect every aspect of the FAA's mission, including AVR's, is the ongoing transition from ground-based Air Traffic Management to an era of Global Navigation Satellite Systems (GNSS) and advanced Communications, Navigation, Surveillance (CNS).. The U.S. FAA has provided consistent and aggressive leadership in all activities leading to this successful transition. The FAA's role started with extensive involvement in the Future Aeronautical Navigation System (FANS) subcommittee of the International Civil Aeronautics Organization (ICAO). Then its role expanded significantly with the RTCA TASK FORCE I, mixed government and industry examination of transition planning and the issues associated with GNSS.

Since that time, FAA's aggressive research and development efforts, as well as AVR's early approval of "GPS Overlay Approaches" and initial passenger carrying airline approaches have continued to show U.S. commitment as well as a responsible transition approach. Later RTCA Task Forces have examined the issues surrounding civil aeronautical data links. Now Task Force III has produced a superb "operational concept" for the exciting and promising subject: "Free-Flight". **In each of these efforts and many more the FAA continues to provide global intellectual leadership.**

There has been only one significant negative factor in U.S. transition to these advanced systems, with their promise of enhanced safety, improved use of the airspace, and operational cost savings for the FAA and the civil and military aviation communities. This negative factor has been the failure of the FAA Advanced Automation System for ATM. The failure of the AAS project has been the principal slowdown in the implementation of modern computers and software for today's ATC infrastructure as well as for transition to a future GNSS, CNS system.

Along with the FAA's research and development efforts, AVR has been a leader and a partner in the process of transition. This is partly due to the enterprising approach by its Associate Administrator, Mr. Tony Broderick and partly due to the thoughtful, open-minded, but still discriminating efforts of the men and women of AVR. However, as the transition to CNS ATM proceeds, an increasing burden of transition certification activities will fall upon the organization. These efforts will require new capabilities and new skills within AVR, as well as increased workload.

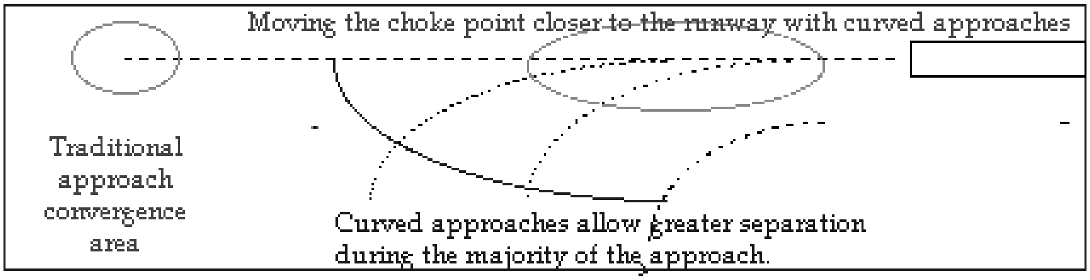
The following section of the report is not intended to reproduce, summarize, or even refer to the many reports, research and operational test results; or to provide a balanced view of upcoming challenges for certification, administration, control and safety for the FAA as it takes the next steps toward CNS ATM. Instead, the subcommittee chose to focus on several specific areas of GNSS and CNS technologies that will significantly impact AVR or will provide exciting new possibilities.

AVR's certification process for GNSS, CNS, and Free Flight for both equipment and procedures is well underway. Some critical examples are as follows: (a) Required Navigational Performance (RNP) has been developed and verified by RTCA Special Committee (SC)-181. (b). A concept for interference mitigation has been incorporated in early receiver designs and verified by RTCA SC - 159. (c) The FAA is exercising its leadership within the ICAO by promoting RNP in the GNSS Panel. (d), On board "Navigation Data Bases" will augment and facilitate CNS systems and standards and these data bases are under development in RTCA SC 181. (e), Standards are under development for GPS Category I, II, and III approaches. And AVR has many other initiatives underway.

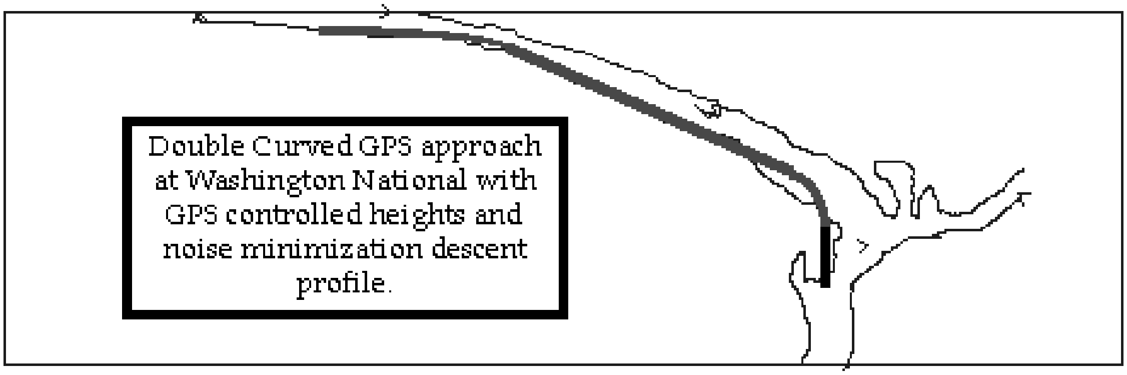
Much of this progress is being made via the internal partnerships between AVR, ARA. and other organizations within the FAA. Progress is also facilitated by the FAA's effective use of Integrated Product Teams [see section II of this study]. Thus, the FAA has been leading in both research and development and in aggressive certification activities.

Some of the results of this new and basic standard setting will offer dramatic improvements in ATM, safety, and efficient use of our airspace! One set of examples will involve the whole panorama of new, curved approaches [implemented with much more flexibility and benefits than the old Microwave Landing System could ever produce]. However, to gain further understanding, air traffic efficiency benefits, and final certification of these procedures by AVR.....will require substantial effort.

Example: Using multiple and concentric curved approaches to a single runway to maintain or increase separation standards while moving the convergence or "choke point" as close as possible to the runway!


Moving the choke point closer to the runway with curved approaches
Traditional approach convergence area
Curved approaches allow greater separation during the majority of the approach.

Example: Consistent and precise "double-curve" approaches and climb outs are possible on the Potomac River approach to Washington National Airport and could become a unique GPS certified approach.


Double Curved GPS approach at Washington National with GPS controlled heights and noise minimization descent profile.

The FAA should not be satisfied with its present, very productive program of "Overlay GNSS Approaches"; because they essentially are *reproductions of old "straight-in" approach procedures and do not demonstrate or explore the full benefits of GNSS.* The Atlantic City Technical Center, NASA Ames, or other FAA and contractor simulators should be able to accelerate the certification of a sample of difficult and unique GNSS operational approaches to get an early view of operational advantages, problems and related ATM issues. These simulator-based certification efforts could be flight checked for safety by certification flight test and the results published for interim use. The "interim" approaches could be used as an incentive for selected operational airlines (and, in some cases, business or general aviation aircraft) by offering ATM priority service for aircraft equipped to utilize these new approaches. Finally, the experience and data gained from these safe, but selectively utilized interim approaches could be used as the statistical data base for final certification. Although periodic flight checks by FAA aircraft would be important to ensure safety, the number of checks and the flight resources to conduct them could be significantly reduced by this "***simulation----check for safety----interim incentive operation----final certification"*** approach. The key to the statistical data gathering that is possible using GPS is as explained below:

For classical, ground-based navigational aids [such as Instrument Landing Systems (ILS)]; landing approach procedures and ground-based ILS equipment had to be periodically flight tested and verified. This was because, even though there were independent means of checking position [radar], the "checkers" never knew exactly what the pilot was seeing on the his instruments [or if the pilot was accurately flying the approach].

As GPS approaches are flown, the aircraft determines its position from the constellation of satellites and transmits that position to other aircraft and to controllers on the ground. *The statistical sum of a group of transmitted aircraft positions, gathered on different approaches by different pilots and different aircraft; should provide a high probability of verifying any approach procedure.* Although instrument errors may occur, a sufficient operational sample should eliminate the bulk of those errors. Thus, this data base of early experience can support safety analysis, the development of pilot and aircraft airspace safety margin needs, airspace and approach efficiency and hazard analysis, aircraft "by type" noise analysis, etc. **Further, this should provide a high probability of significantly reducing dedicated FAA flight test activity, thereby saving both verification aircraft and personnel resources.**

A "human factors" issue for the future will be the description of "Tunnel concept" instrument approaches as well as the transition from higher altitude free flight operations to an approach or landing queue for an airport. Either of these could be very different from "centerline-in-the-sky" procedures previously used and supported by ground-based navigation aids or radar. "Tunnel" procedures, if they are used, will have to be described differently on approach plates and portrayed differently on cockpit instruments. The operational advantages or disadvantages of "tunnel" approaches as well as the human factor issues for approach plates, instrument portrayals, and pilots have not yet been fully explored [although a great deal of discussion and analyses have been performed during RTCA committee meetings, and as part of GPS flight test programs].

All aspects of the "tunnel" concept---the flexibility, the portrayal, the human factors, the size and specificity of the "tunnels", and many other issues associated with using a different approach for the critical transition from "free flight" to the necessarily more restricted landing phase of flight need additional analyses, simulation, and flight test. The same issues must be addressed even if the transition and approach does not utilize "tunnel approaches", but merely address the transition from free flight to efficient queuing for curved or straight in approaches. Again, extensive simulation, selective "early operations, and statistical data gathering from those operations will assist in the description and certification of those critical flight procedures. **The "tunnel" concept will be only one of a series of very subtle human factor issues that must be fully explored as the FAA begins to introduce a full "free flight" regime for certification and for operations.**

As the role of the air traffic controller moves from that of "controller and director" to that of "safety monitor and airspace manager", the relationship of the controller to the pilots in the cockpit needs careful *human factor analysis.* For example, a prime cause of accidents on training flights, is the “gray” period where the trainee has direct control of the aircraft....then as a trainee begins to get into trouble the situation can move into the “gray”zone (where the instructor is giving the student some extra time and margin to “see if he can get himself out of it)....but if the instructor allows the student to go just a small distance too far....it becomes too late to recover. **The future “authority relationship” between aircrews and controllers as air traffic managers has the same potential for “gray zone” accidents; and both pilot and controller will need assistance to avoid accidents of this type.**

In a “free flight” regime, both the pilot and the controller will have the benefit of *new software tools* to assist air traffic conflict and authority judgments; an example will be the use of “protected zones” and “alert zones”. But if the pilot does not respond both properly and quickly to maintain separation, what process does the controller use to advise or direct the pilot and how simply does the controller return responsibility to the pilot after assuming control? This process is straightforward where distances are great and conflicts develop slowly, but as aircraft converge toward runways and at certain high traffic points, the human factors become much more significant. *Hence, the need for significant simulation and flight verification of this process, as well as the human factors involved, the difference that various display parameters can make, the use of automated voice or display alerts, and many others.*

The FAA should also investigate full, simulator based, human factors studies of the many and subtle interactions between pilots, aircraft instruments and displays, air traffic controllers operating in the ATM mode, and the effects of their displays. This study needs the IPT approach and the full involvement of both Air Traffic controllers and researchers, AVR, the R.&D. capabilities of the FAA, DOD, and NASA as well as industry and academia.

In addition to full simulators, which (if properly designed) can provide very effective human factors information, there are more specific simulators which will simplify and accelerate investigations of key phenomenon, and determine safe U.S. operating procedures, etc. Other examples are as follows: a simulator that allows flexible insertion of smoothing and tracking filter designs; or a simulator that models various “Automatic Dependent Surveillance” communication protocols.

Special use communications performance simulators can be used to investigate ground receiver locations; others could simulate radio-link interference models; or could be used for various runway congestion tests, etc. With these specialized vehicle, communications, or other part-task simulations we can verify software algorithms, determine safe and more optimistic separation standards, and optimize other equipment parameters for certification. *The development and support, of this family of specialized simulators is more an industrial and R&D responsibility than that of AVR. The FAA and its community of university and industrial centers of excellence is already providing important simulation research as well as early development of operational parameters.*

Nonetheless, simulation technologies, standards, and certification issues will not remain constant over long periods of time. There will continue to be new technologies for evaluation as well as the need to provide a methodology for smoothly transitioning these technologies into an evolving, global ATM system! Thus, these specialized simulators should be mostly located in academe or in commercial industry and utilized on a contract basis....(to minimize capital investment and the continuing costs to modify and upgrade special simulations for new tasks or new technologies and to amortize training costs). Industry will also need access to these simulations. Thus, it should be possible to spread ongoing costs across both FAA and industrial users.

There are many other related issues that should be discussed in this section, advocating the benefits of advanced simulation—especially for GNSS, CNS, and Free Flight, but the discussion above outlines the range of issues. Issues such as the value and use of “Integrated Product Teams” and better exploration methods for “Human Factors” are discussed in more detail in Section II of this report. Finally, it must be re-emphasized that these simulations require multi-disciplined people, and vested organizational involvement by several of the key agencies within the FAA [including AVR] and many cooperative facilities and operations that are extant in the Department of Defense and in NASA.

R-3: TO ACCELERATE THE NEXT PHASE OF CERTIFICATION OF ATM PROCEDURES FOR GNSS, CNS, AND FREE-FLIGHT AVR SHOULD INCREASE THE USE OF STATISTICAL DATA SAMPLING AND SIMULATION FOR FLIGHT PROCEDURE CERTIFICATION--- WHICH CAN ENABLE REDUCED FLIGHT CHECK PROGRAMS. A WELL STRUCTURED EFFORT COULD INCENTIVIZE EARLY AIRCRAFT EQUIPAGE AND SAVE RESOURCES FOR THE FAA.

ADDITIONAL ADVANCE TECHNOLOGY ISSUES

This section of the advanced technologies report is primarily a **"hardware oriented"** set of specific, individual technologies that will also challenge traditional certification, specification and other FAA control processes.

One of the most promising structural technologies that has already been investigated by the FAA, NASA, the aviation industry, and the military services is **the field of composite structures**. We already have nearly 30 years of aviation experience with composites of different kinds: including specialized panels on commercial airliners; pioneering full aircraft structures for smaller, general aviation aircraft and one major business aircraft; horizontal and vertical tail assemblies on hi-g fighter aircraft; experimental composite wing structures for transport aircraft and one forward swept wing fighter; and recently—full aircraft structures on specialized aircraft for the military. This range of experience is also being extended by composite rocket structures and hot section components, automotive body experience, composite patches of different kinds, and many other industrial plastic and composite applications. This base of experience allows us to realize that their are few "mysteries" left in this exciting field, but there are still problems.

For example, fundamental composite structural design models rely heavily on idealized results from basic manufacturing processes. Unlike the well defined test and aging criteria for aluminum structures, [which utilize well established "crack growth criteria”] the performance of composite structures is highly dependent on laydown patterns; the purity and care with which chemical adhesives are handled; careful attention to curing temperature profiles; etc. Additionally, there are still substantial inconsistencies with the performance of different fastening techniques—i.e. the combination of adhesive bonding with metal supplemental fasteners for reliable horizontal tail structures, composite skin bonding to a typical titanium spar structure—and many others.

These differences from experience with aluminum structures continue through the operational lifetime of the aircraft—i.e. well assembled composite structures should not corrode like aluminum structures do, but they are affected by oil spills, certain types of de-icing fluids, etc. Thus, the broader process of certification, maintenance tracking, aging, related inspections.....all these processes require a system approach from requirements setting with proper margin of safety modeling, the margins for uninspectable manufacturing and assembly faults and the difficult projection of environmental effects, random human error, etc.

It must be noted that composites have been under evaluation for decades and throughout this period all the key governmental and industrial players have been involved. Additionally, the cost competitiveness of composites with conventional aluminum structures has been gradually improving, but with the exception of specialized panels and components this cost equation has only recently shown that composite primary structural elements are economically viable. Airbus Industries has now certified two primary structure elements. Many members of the committee believe that U.S. coordination has been excellent through the extended transfer process for this technology. With the exception of the resolution of several key issues on boron-epoxy patch technology, **there is a general consensus that this technology development process is one that is a deliberate and effective progression for the FAA, NASA, the DOD, and industry over a very long, but productive period of time!** Nonetheless, as composites begin to move into the realm of primary structure for subsonic air carriers and will eventually include the challenge of the high speed civil transport, there are remaining issues that continue to warrant priority, inter-agency attention.

One of the principal remaining problems is that there are few effective non-destructive test techniques that can provide substantial confidence to the quality and effectiveness of initial production processes while also providing understanding and comfort associated with structural aging! Additionally, there are a lack of effective test techniques to measure allowable levels of working stress and relate the low levels that are presently used to a repeatable theory of material properties. Further studies of fatigue spectrum effects are required, and *again the FAA should be commended for innovative research and the development of a load enhancement factor approach to the certification of GE-90 fan blades.* Finally, a composite assembly has more design variables and more failure modes than conventional metal construction and is unduly penalized by the concept of “worst case design”. Thus, more work is required into the use of “probabilistic design” as an alternative to “deterministic design”.

Therefore, both more R&D and more certification work for AVR is required ahead. Fortunately, the experience base with full composite aircraft structures and major components is expanding very quickly. The military B-2 bomber, the F-17 fighter, the Beech Starship, several all composite light aircraft designs---*and they should provide substantial data on which to base accelerated and broader certification of new applications and new aircraft in the future. these are all a rich source of design, manufacturing, test, and lifetime support experience.*

Even with all our expanding experience in composite structures, it should be recognized that **we are in the process of changing paradigms from metal aircraft to composite aircraft. This transition is as profound as the historic change from “wood-wire-and-canvas” to metal aircraft that occurred in the 1930’s.** The fundamental nature of this change, along with the many issues and possible benefits described above, suggest that a special composites certification inter-agency Integrated Product Team (IPT) should be considered; further, this IPT should be supported by a dedicated Scientific Steering Committee. Further, the special simulation discussion (above) is critically relevant in this area of technology. The relationships between design models, manufacturing margins, testing, and operational experience are so critical that the development of special composite material properties simulations as well as probabilistic design simulation techniques will be an important capability for the FAA, NASA, the DOD and U.S. industry for the future. *Therefore, very high priority should be placed on the rapid development of additional composite analyses, testing, and simulation capabilities for continued U.S. technological leadership in this vital area for aircraft structures.*

Finally, individual agency and industry plans should be further coordinated to develop an accelerated “Composite Verification and Certification Master Plan”. This should encourage industry to invest further, because they will have added confidence that all agencies of the U.S. government with both development and regulatory responsibility will act together to provide scientifically consistent and predictable certification requirements and schedules....a regulatory pull for industry, but one that does not get out ahead of industry needs. This plan should include the topic of composite patches, as well as composite components, panels, and primary structure initiatives. This process should be a logical extension of the planning and work which is already well coordinated.

Process predictability is particularly critical: if the management of technology companies feel their investment in research and development for certification has known requirements and predictable schedules...they will invest when the business case warrants. If industry does not have that confidence: it would signal the end of new technologies for the aviation industry. *Further, if the process within the U.S. FAA [which is clearly the agency of choice for initial certification of technologies proposed by U.S. companies and many international companies as well] was anything less than aggressive, scientifically enlightened, and predictable—then U.S. technology would quickly migrate abroad and the FAA would lose its world leadership role in this area.*

R-4: AVR SHOULD ENHANCE ITS ALREADY EFFECTIVE PROGRAM OF GATHERING DATA AND ENHANCING CERTIFICATION FOR COMPOSITE STRUCTURES BY WORKING CLOSELY WITH OTHER KEY AGENCIES AND INDUSTRY TO DEVELOP A DETAILED AND ACCELERATED, OVERALL INTER-AGENCY "MASTER PLAN" FOR VERIFICATION AND FLIGHT CERTIFICATION OF COMPOSITE TECHNOLOGIES. THIS SHOULD INCLUDE INTENSIVE DATA WAREHOUSING FROM ALL OPERATING ENTITIES THAT FLY AIRCRAFT WITH COMPOSITE COMPONENTS.

OTHER ADVANCING HARDWARE TECHNOLOGIES

There are key hardware technologies that are bursting on the commercial world of consumer electronics. One of these that is also impacting the field of civil aeronautics is the Head Up Display. Head Up Displays (HUD's) have been used in military fighter aircraft for a long period. Their functions were to provide the pilot with complex and fast moving information while allowing the pilot to maintain his view of the outside situation. HUD technology is proven, and now—it is being utilized in several commercial airline fleets, notably Alaska Airlines, Continental, etc. The Alaska flight crews give the HUD the same high marks as fighter pilots around the world. Unfortunately, it is an expensive technology. As it progresses, lower cost versions of the traditional aircraft HUD may be developed for aircraft, but it will take moving to the newer field of "automotive HUD's" to reach an affordable level for general aviation aircraft. Automotive HUDs are available now at a cost level of several hundreds of dollars (exclusive of retrofit and other system costs).

Similarly, flat panel displays have been available for lap-top computers for years. Further, new versions of flat-panel systems are coming which will be larger, cheaper, and offer much higher resolution than today's computer displays. One advantage of these future systems will be their ease of installation on new aircraft and their possibilities for retrofit on older aircraft without completely rebuilding existing instrument panels. Both of these commercial technologies will be particularly important as the general aviation fleet faces the prospect of dealing with a GNSS—CNS environment which can offer enhanced safety and simplified flight operations through effective presentation of massive amounts of image data to flight crews as well as other information.

These technologies can also be synergistically utilized with simple aviation qualified versions of commercial computers—such as “laptops” or “Newton type devices” However, the utilization of these commercial technologies, raises the issues of COTS electronics developed for a much less demanding environment and the issues of COTS software [discussed above and dealt with in detail in Section II of this report]. Again, the good news is that reliability levels of these commercial products are already very high, the devices are designed to operate in difficult environments (but not to the broad range of environments required for on-board aviation equipment), and the development and manufacturing processes associated with these hardware items are subjects of intense competition and rapid improvement. The clear specification shortfalls for use of commercial equipment in aircraft are high and low temperature operational limits, electrical and RF interference limits, pressure ranges, human factors issues, and several others.

The FAA should examine with industry, likely commercial electronics equipment for aviation use to determine what categories of upgrades would be required for safe and effective use of these devices or their derivatives. This review might include FAA specialists, representatives of the ATA, the general aviation community, traditional aircraft electronics manufacturers, and representatives of the commercial products under consideration.

One consideration during such a review is whether or not there can be a gradation of standards for safe flight operations. These graded categories would revolve around such issues as the following: are the equipments a hazard (i.e...is it in a single-string where failures would damage flight safety critical equipment)?---

and is there an adequate level of redundancy for critical or for "nice-to-have" functions?---and many other questions that represent long established practices, but ones which could be reconsidered for certain categories of equipment.

Additionally, the review should consider various levels within the vertical or integration ladder of these devices....i.e. consider if a single standard, commercial, integrated, circuit chip; or advanced memory device is acceptable if sufficient redundancy is available and if the devices are conformally coated to meet aviation pressure and electronic discharge requirements. Similar consideration could be given to higher level circuit board assemblies....i.e. Perhaps a commercial flat panel display is acceptable, if it is configured in two halves—both would normally be used to present a large map display or weather information. The concern would be if there were a significant failure.

However, with the exception of overall control circuits, a failure could occur which affected the display, robbing the pilot of safety critical flight information. However, if redundancy were inherent in the display (i.e. if halves or quarters were independent) then the independent section could continue to operate at a reduced image size. There are many other redundancy schemes that can be applied at all levels of electronics design, and these issues should be an inherent element of the recommended review. *The potential for upgrading promising items of commercial electronics equipment (originally designed for ground operation) could be so important to the continued development of airborne avionics that policies and certification issues associated with those upgrades should be carefully reviewed and guidelines established.*

R-5: AVR SHOULD INVESTIGATE THE ISSUES ASSOCIATED WITH UPGRADING COMMERCIAL ELECTRONIC EQUIPMENT SUCH AS COMPUTERS, DISPLAYS, AUTOMOTIVE HUDS, ETC. IT MUST BE RECOGNIZED THAT THESE ITEMS WERE DEVELOPED FOR NON-SAFETY CRITICAL USE ON THE GROUND, BUT THE BENEFITS FOR AVIATION USE OF THESE RAPIDLY ADVANCING ITEMS OF

TECHNOLOGY WARRANTS A REVIEW AND THE POTENTIAL DEVELOPMENT OF GUIDELINES FOR AVIONICS UPGRADES.

Another fundamental area of rapidly improving hardware technology is the field of **Advanced Sensors.** These could fall into several categories. For example, one class of highly useful sensors that has already been investigated and flown (and mentioned briefly above) is the category of equipments for "Synthetic Vision" Several electronics companies have developed, tested and some, partly certified, both microwave sensors and infra-red sensors for aircraft. The target market was primarily air transports, and the primary application was to assist in low-visibility landings. An added benefit was to be of assistance for taxiing during very low-visibility periods. These systems have been tested and proven their worth, but their implementation is slowed by both airline demand and by effective completion of practical certification.

A different category of sensor for airport operations enhancement is the GPS "Squitter" which has been substantially tested at the Lincoln Laboratory and Logan Airport in Boston. The GPS "squitter" can easily provide total traffic management capability [including both aircraft and vehicles] at reasonably low cost.

A completely different category of sensor, which is much further in the future, is the "smart sensor" which could be built into aircraft structures so the structures themselves provide direct health or usage data. An example of this concept is to build strain gauges directly into critical locations of a new aluminum wing structure. The potential of these types of built-in sensors for composites should also be carefully examined. Such sensors could be included in all aircraft, or only in "lead-the-fleet" aircraft, which would then be in a much better position to provide more accurate and complete stress and fatigue information than today's count of simple "cycles" [take-off, climb to cruise altitude, descend, and land].

There are other sensors that are used extensively today for self-test of electronic components. Or they can be used to provide completely different applications than originally envisioned. A superb example of this dual use, is the experiment conducted by a team at Stanford University that placed dual GPS receivers in the wingtips of a light, general aviation test aircraft. In addition to GPS location functions, the wingtip installations allowed the GPS signals to become a backup artificial horizon as well as provide measures of the "wing-flex" during the test program. *The technology of advanced sensors for aeronautical use is advancing and will in the near future provide enhanced methods of improving manufacturing methods; extending the knowledge of design and testing limits from original manufacture throughout the operational life of an aircraft or its components, and finally to extend the capabilities of the pilot....all of these should significantly improve safety!*

R-6: AVR SHOULD CONTINUE TO EMPHASIZE TECHNOLOGY ADVANCES SUCH AS NEW TYPES OF ADVANCED SENSORS FOR RELIABLE MANUFACTURING, FOR PROVIDING INTIMATE DATA ON THE STATE OF EQUIPMENT AND AIRCRAFT, AND FOR NEW TECHNIQUES OF EXTENDING PILOT CAPABILITIES.

AVR already has a clear, defined and highly effective regulatory structure for certification, that must be commended both in its content and application. However, this structure should include a consensus approach for identifying safety-critical items and a methodology for encouraging industry to accelerate their development of safety enhancing products, with the full cooperation of any and all interested agencies of the government and the aggressive support of AVR's certification teams.

This "verification methodology and certification pull" should be so compelling for safety enhancing items that both the industrial and financial communities would find the business case for these items to be "irresistible". AVR should re-examine it's policies, organization, and regulatory structure to see what should be done to create this "Safety Compulsion" atmosphere for the American aeronautics industry!

R-7: THE FAA SHOULD REFINE ITS CAPABILITY TO IDENTIFY NEW TECHNOLOGY AREAS THAT COULD HAVE AN IMPORTANT ROLE IN REDUCING FUTURE ACCIDENTS (I.E. MANY OF THE MEANS DISCUSSED IN THIS REPORT). AVR CAN ASSIST BY EXAMINING ITS REGULATORY PROCESS WITH THE GOAL OF CREATING A "COMPELLING" PROCESS TO HELP INDUSTRY CREATE "IRRESISTIBLE TECHNICAL AND BUSINESS" INCENTIVES TO DEVELOP AND CERTIFY PRODUCTS TO ENHANCE SAFETY IN THOSE IDENTIFIED AREAS.

To create this kind of magnetic atmosphere without "getting ahead of industry" or falling into the industrial policy trap of "picking winners and losers" is a difficult balancing act. However, such a review should carefully consider, but not be limited to the following:

- The data base of accident causal factors should go beyond the first and second order factors outlined by the National Transportation Safety Board (NTSB). There must be a methodology for examining accident causal factors and categorizing them at a higher and more subtle level. Properly categorized accident data, amplified by incident data should provide a "problem---and accident potential" structure that could be prioritized and made available to industry for possible solutions. The "data warehousing" recommendation (R-l above), could assist in the analyses and development of this prioritized listing of needed safety solutions.

- Once "problem areas to be worked on" are identified or categorized, then effective techniques for communicating these problem areas to industry are needed. This activity needs to be one that is not related to the normal FAA procurement process, but does ensure a fair and easily accessible method of understanding the safety potential problem area.

- This may be sufficiently critical that partial funding from one or more agencies of government would be possible. This implies establishing an undefined "safety budget" line item. This could be within the FAA, NASA, DOD, or even DOT budgets. Or it could be more indirect in the “trust fund”, or include guaranteed loans for small business, etc.

- Finally, this “safety-pull” for selected items for development and certification may require a special “action team” within AVR, and interim demonstrations, or support via FAA conducted simulations and flight tests, etc. It would also require special review procedures to evaluate both progress and continued pertinence to safety enhancing potential. At the least this “pull approach to certification” would require the development of specific criteria.....and it would require a discriminating means of ensuring that all other categories of efforts undergoing development and certification are not classified as “less important, or safety neutral, or worse---safety is not important.

The above issues may be so difficult that this recommendation is impossible to implement. Nonetheless, the safety imperative is so important for the future, that the committee felt it important to ask that this recommendation be considered!

SUMMARY OF SECTION ONE OF THE REPORT

ADVANCED TECHNOLOGIES, has concentrated on the impact of several key technologies on the critical FAA functions of certification and other processes of enhancing safe and efficient aviation.

The fields of advanced information and advanced simulation should have the greatest impact and the greatest benefits on these critical FAA activities. The recommendations in those subsections of the report are designed to initiate major new thrust areas, or to re-invigorate and expand areas in which the FAA is already constructively engaged.

The FAA’s leadership in the global movement to GNSS and CNS air traffic management has been something this nation should be particularly proud of, and we should all look forward to cost savings as well as improved operations. The recommendations in this section are limited in scope because numerous previous studies have outlined important initiatives that would only be redundant if re-iterated here. However, the recommendations do focus on accelerated efforts in certifying new approaches and other means of accelerating implementation of CNS.

Finally, the section focusing on a selective group of hardware technologies that will also contribute to the ATM revolution as the next decade opens up additional areas for FAA exploration and action.

The last recommendation to create a compelling “safety-pull” for R&D and for certification needs careful evaluation, because it implies another operational paradigm for AVR and difficult trade offs for certification.

SECTION II---THE IMPACT OF NEW TECHNOLOGIES ON SYSTEMS AND DISCIPLINES

This section of the subcommittee report addresses the disciplinary issues associated with complex systems made up of other systems. For safety critical applications of these complex systems, the disciplines and their consistent application is the key to reliable performance. The first discipline is the application of Human Factor research and methodology and new technologies that can enhance disciplined methods of improving safety and certification processes.

HUMAN FACTORS IN SAFETY CRITICAL APPLICATIONS

BACKGROUND: Human Factor disciplines and methodology are a set of tools which should be used in the design process, the testing process, and on a continued evaluation basis through the operational phase of a system. That system may be an aircraft, a Traffic Management System, a pilot or maintenance specialist training system, or many other areas that require interfaces between human beings and equipment.

While the tool sets include anthropometry, physiology, perception aids, rapid prototyping tools, simulators, discussion sessions, performance tests, and many others....most of these are either mechanical operation applications or careful examinations of a cognitive process or both.

For aircraft development, the application of Human Factor research and methodology has had three principal themes: In the 1960's and 70's, "crew workload" was one principal area of attention. Of course, the issue was safety and crew performance, but there were other motivational factors as airlines were also looking to safely reduce standard crew sizing. In the 1980's "situational awareness" became a significant concern. And in the 1990's, attention has gone beyond awareness to "human error and mode awareness". Although there was also clear attention to human factor issues for the private and business flying public, the amount of human factors research effort at this end of the aviation spectrum has not been the same.

As an instructive device for the applications of human factors research in aircraft design it is helpful to briefly review the philosophy used by Boeing for new aircraft, including the development of the Boeing 777. First, the company uses a well established and fully articulated design philosophy for the flight deck, and from this flows a well researched set of applications implemented into the cockpit design.

SELECTED EXAMPLES OF FLIGHT DECK DESIGN PHILOSOPHY:

a. The pilot is the final authority.

b. Both crew members are ultimately responsible for the safety of flight.

c. Design for operations based on pilots' past training and experience.

d. Design systems to be error tolerant.

e. The design hierarchy is---simplicity, redundancy, and automation.

f. Other equally important guidelines.

SEVERAL EXAMPLES OF DESIGN FOLLOWING THE PHILOSOPHY:

a. Flight controls linked from left to right.

b. Flight controls backdriven to reflect autoflight systems commands.

c. Envelope protection is overrideable by the pilots using familiar control.

d. Electronic checklist display is manually selected to ensure pilots are in charge of when the checklist is run.

e. And many others, all vital to safe flight deck operations.

EXAMPLES OF ISSUES IN SAFETY AND HUMAN FACTORS

a. The right level of airplane autonomy for free flight.

b. What information and controls does the pilot require?

c. How will ATC and the aircraft operate in both old and new ways during the transition to free flight?

d. Future uses of TCAS (not presently anticipated) are highly likely.

e. Predictive wind shear systems and their relationship to reactive systems.

f. The difficulty of assigning probabilities to human error for part 25.1309.

g. Suppliers sell equipment to airlines under Supplemental Type Certification processes that do not fit the original flight deck philosophy.and other important current issues

NEW TECHNOLOGIES WILL AFFECT HUMAN FACTOR WORK

The above lists were intended to focus the reader’s attention on the current state of human factor philosophy, tools, implementation and issues. This section of the report is not aimed at solutions to these issues—that is a matter of research and many critical efforts. However, there is an important final perspective: *The overwhelming majority of aircraft accidents are primarily or secondarily the result of human error! The human operator, mechanic, or support person, the designer, the specialist working on the* *manufacturing floor...all of these are the least predictable element of the aeronautical system of systems! We have made great strides in human factors research....but now the challenge for the goal of "near-zero accidents" for the future is how to translate all we know about human factors into repeatable science and practice.*

The FAA and AVR have an effective and well coordinated human factors plan with the DOD and NASA, and this area is worked extensively with civil academic and industrial assistance. However, the accident rate speaks for itself---we are not doing enough, nor are our efforts sufficiently effective! We would like to be able to examine the human participants for undetectable errors as we might apply "crack-growth theory to manufacturing of metal components. We would like to be able to design the human participants role, training, and performance in the same way that we check tooling for tolerance during manufacture and electronic components' performance during flight. We *can* think about the human capacity for progressive performance over the years with the same interest and care that we use to follow the aging process for an aircraft structure (provided we remember that human aging also includes improved judgment and the capacity for non-linear performance).

The first step is to apply more resources and more expertise to the human side of the aeronautics industry. The second step is to ensure that these extra resources are specifically aimed at targets that will make a real difference in performance and dramatically reduce accidents.

There are some advancing technology tools that can assist in this specific process---in particular, the broad use of simulation in every aspect of aeronautical design, manufacture, operations, and support is one of our most effective tools. The increased use of advanced simulation has already been mentioned in Section I of the report. In some cases, one thinks of the incredible flight simulators that can be used for training, but can also be used to ensure excellent human factor considerations in the design of a new aircraft.

Sufficient numbers of these simulators exist today and are used with superb support staffs of training experts, human factors experts, pilot pools for experimentation, etc. In some cases (the FAA Technical Center and NASA Ames), these realistic flight simulators are tied-in to excellent ATM system simulations, so that the interaction between flight crews and air traffic controllers can be carefully studied. *The subcommittee believes all these capabilities can and should be used to the maximum extent as we move into the new era of GNSS, CNS, and Free Flight.*

However, there are new technologies and advances in traditional simulation technologies that should also be seized upon. For example, “Rapid Prototyping” has reached a new level of maturity with very capable and flexible computer hardware and displays; augmented by advanced “object oriented” software tools, and simulation programming methodologies; and supported by teams of experts in the art of quickly creating prototype simulations with targeted realism (i.e. “only where needed to obtain valid results”).

This capability will soon be enhanced with “virtual reality” glasses and other support technologies such as 3-dimensional displays. These special capabilities exist in several commercial companies, in several “system integration” contractor facilities, and in several government locations.

“Rapid Prototyping” *will serve to enhance and focus human factor studies, while offering the possibility of quickly modifying the design of equipment to adapt to the findings of the prototype effort.* Further, with some encouragement and investment, several of these facilities could be tied together to provide specialized added capabilities, or to provide easy access to a different pool of human operators to be tested. This is already being done, but the efforts can be increased, particularly as they provide a low-cost method of expanding human factor disciplines and application work as we move into a new era of ATM. This expanded effort can be funded by several agencies and shared with private industry. Because these kinds of facilities are in high demand, it will be imperative to find ways to provide priority to the FAA.

R-8: AVR (THROUGH THE FAA R&D ORGANIZATION) SHOULD EXPAND FULL SIMULATION AS WELL AS "RAPID PROTOTYPING" HUMAN FACTOR STUDIES TARGETED AT AREAS IDENTIFIED WITH "HIGH ACCIDENT POTENTIAL" AND ASSOCIATED WITH EQUIPMENT AND PROCEDURAL CERTIFICATION. THIS EFFORT SHOULD BE WORKED JOINTLY WITH NASA AND THE DOD.

An additional technology that will have a significant effect on human factor research and on the application of results of human factor simulations is a new regime of*"simulation support software"(SSS). This support software can be used to provide a different insight into simulation data and to focus on the "last percentage point" of human error and cognitive or mode failures.*

As David Hinson noted at the Aviation Safety Initiative Review in December of 1995, "Breaking below the current plateau of flight safety will take a....concentration of effort. Achieving zero accidents calls for a new paradigm, a new approach".

In the past, human factors simulations provided so much complex data, that it had to be summarized....and one principal focus was on "majority behavior or majority errors". In other words, the data was often so subjective or complex that it was nearly impossible to focus on individual failures or cognitive problem areas. Instead it was primarily a calculation of modes and means and normal curves.

In contrast to this approach, **software test programs** keep track of exactly how many times a programming "branch", or an algorithm was used and how many times and *why did any individual failures occur! With advanced SSS, it will soon be possible to utilize these software test techniques on human performance.* It should also soon be possible to isolate the human "mental algorithm" which failed by isolating the event with a combination of fault tree software and interview techniques.

These software possibilities are only in crude form today, but they can and will be enhanced if there is a real demand. It could provide a significant advance in human factor engineering to be able to isolate the "one-in-ten thousand" failure mode and to connect it to the cognitive failure as well as to the timing and circumstances surrounding the failure. With an array of several of these advanced software tools, and with ***data warehousing of a broad array of human factor simulation results*****.....we may indeed be able to approach the Administrator's goal of a new paradigm to tackle the human factor aspect of the accident plateau.

R-9: AVR (THROUGH R&D) SHOULD EXPLORE NEW SIMULATION SUPPORT SOFTWARE IN CONJUNCTION WITH OTHER CIVILIAN AND GOVERNMENT AGENCIES, VITALLY INTERESTED IN HUMAN FACTOR RESEARCH. THEY SHOULD HELP MATURE THE BEST TOOLS TO DEAL WITH SAFETY, CERTIFICATION, AND TO SUPPORT PREVENTION EFFORTS FOR "NEAR ZERO ACCIDENTS".

Some additional areas of concern to the subcommittee were the following: FAA "human factors" inputs to design must be earlier; and there is a lack of means to quantify FAR part 25.1309 human error issues; the FAA needs to make heavier use of industry simulation capabilities; and the FAA needs more expertise in human factors.

Finally, there is an additional area for human factors research which complements simulation. Simulation will only be effective if pertinent data and information is extracted from the results of the research. This similarly applies to a sufficient understanding of incident reporting and the use of opinion polls as additional means of categorizing problems and pointing to areas of "high accident potential". The techniques for this type of interviewing are well known, and extensively used in human factors research. However, it should be possible to extend these activities to obtain "full debriefs" of incidents, to "fully explore" the best judgments of flight crews and maintenance crews, and to use this information in conjunction with simulation results to **help point to these areas that *require effort to avoid a possible accident in the future!*** *Once again, it is the compilation of opinions, incident interviews, and simulation results that can help in this difficult arena. To properly compile and then selectively access these human judgment data bases, modern "relational data base" software and developing "search agent"* *software can provide great insight .....if the information is properly warehoused for selective access and use!*

Summarizing the above, to prevent future accidents a subtle shift of emphasis is required. Classical human factors research is always vital...but accident prevention comes from clear applications of human factors philosophy, and task oriented design and test. Simulation tools, new software programs, improved interview and opinion surveys all work in conjunction with each other to help avoid the "combination of cognitive and mode problem areas" that are the root cause of many accidents. AVR is in a unique position to facilitate industry, academia, and government efforts in this area.

R-10: AVR--IN COMBINATION WITH FAA R&D EFFORTS, WITH NASA, DOD, INDUSTRY, AND ACADEMIA--SHOULD EXPAND THE USE OF INTERVIEWS AND OPINION POLLS THROUGHOUT THE AVIATION INDUSTRY TO CREATE A BETTER MEANS OF PROJECTING THE POTENTIAL FOR FUTURE ACCIDENTS. THIS DATA SHOULD BE COMBINED WITH SIMULATION AND SELECTIVELY USED THROUGH INFORMATION WAREHOUSING.

EXPANDED USE OF COMPUTER BASED TRAINING

There is a different kind of simulation, which is exploding in industry ---which is not very useful for human factor research, or human factor support in design, but will benefit greatly from both of those activities. "Computer Based Training (CBT)" is being used and will increasingly be used for all types of industrial and machine centered training. An example from the automotive field can illustrate the benefits: General Motors recently conducted a controlled test of "CBT" training for their operators of plastic injection molding machines. These are huge machines, which are very expensive....and training was primarily classroom oriented with written tests, etc. Because the machines were operated 23 and a half hours per day, there was little opportunity to get on-the-job experience, except to "watch over another operators' shoulder". The CBT was a simple computer-screen only simulation, with pictures of the movements of the machine, diagrams of what was going on inside, and images of the controls (utilizing commercially available touch screens). In a short time, the CBT was built using a standard “work station”, and the test scores and general performance of the new workers increased in a major way. As a final bonus, the trainees were able to train on emergency procedures....something that was never allowed on the real machine, because of the risk to the machine and to production.

Computer Based Training is only one of a variety of new and exciting training media: others include special tapes for home viewing, computer and interactive television “training games”, etc. The value of these technologies are their graphic lessons, their convenience, and simple distribution systems. Commercial industry is leading the way in the creation, sales, and use of many very attractive CBT and Taped learning products. *The FAA should encourage their use....use them within the FAA....and should try to ensure that CBT and taped or game products are focused on the real issues that can help avoid accidents in the future.* As discussed above, the great preponderance of objective evidence is showing that these learning products succeed. **In an exciting way, CBT and other learning products can be a most significant delivery mechanism for human factors applications to help prevent accidents.**

R-11: FAA SHOULD UTILIZE EVERY OPPORTUNITY TO DEVELOP AND USE “COMPUTER BASED TRAINING FOR ITS OWN PEOPLE, AND ENCOURAGE ITS USE IN AVIATION. AVR SHOULD FIND WAYS TO USE CBT TO DISSEMINATE CRITICAL HUMAN FACTOR LESSONS TO HELP AVOID ACCIDENTS.

EXPLOITING THE BEST OF INTEGRATED PRODUCT TEAMS

This topic area does not represent an advanced technology. Further, the topic deals with a management philosophy which is already in use within many parts of the FAA, including AVR. However, the results that well-trained and balanced “Integrated Product Teams” (IPTs) can achieve have been so dramatic in most places that the subcommittee felt compelled to complement the FAA on the results they have achieved to this point. And they wish to point out that IPTs can be utilized even more broadly in the certification and safety enhancement process.

Rules for success within IPTs are simple and well known---but some of the principles are as follows: cooperation is essential; full and open access, no secrets; each member brings unique expertise to the team; open discussion does not mean that each viewpoint must be acted upon; ownership is vital; the IPT does not replace the program or certification manager..the team advises and explores; empowerment of the IPT by management is critical; continuous communication.

The advantages of a broader IPT process for AVR are potentially---better decisions, more timely action, more open criteria, and standard processes for external customers. Internally, improved and expanded IPT operations should be less bureaucratic, allowing parallel processes to work effectively...rather than serial ones, and broader expertise can be applied to difficult certification issues on a more consistent basis.

R-12: AVR SHOULD CONSIDER BROADER APPLICATION OF THE INTEGRATED PRODUCT TEAM APPROACH TO CERTIFICATION.

TECHNICAL EXPERTISE AND NATIONAL RESOURCE SPECIALISTS

An additional observation is required from the subcommittee: The pace of technology is now moving so fast, and new technical developments need to be carefully considered on a constant basis. Further, no government agency or commercial company is able to keep up with these fast changing developments. However, technology is the life-blood of aviation and ATM. Therefore, the FAA and AVR needs to utilize every means possible to broadly enrich their technical expertise, both in-house and externally. In some areas, where proprietary information is not involved, external experts can be called on. However, *AVR—in particular—needs wide ranging, internal, technical expert support. The FAA*

National Resource Specialist program is an ideal vehicle to obtain more of this specialized technical assistance and AVR should expand its use to attract and retain outstanding technical capability in many fields.

R-13: AVR SHOULD HIRE MORE NATIONAL RESOURCE SPECIALISTS TO INCREASE IN-HOUSE TECHNICAL EXPERTISE.

COMMERCIAL OFF THE SHELF (COTS) SOFTWARE

The single most significant “system of systems” issue for the modern information age is the accelerated use of Commercial Off The Shelf (COTS), computer hardware and software for complex systems of all kinds. Complex systems which were previously designed from the ground up for a single application, appeared to have the advantage of a highly focused requirement and optimally developed software to operate the system. Unfortunately, the systems have often cost a great deal in development and even more in operations. One of the principal issues for certifying one of these systems for safety critical applications has been the problem of not being able to test every combination of events in a large system. In the COTS environment, there is a much higher probability that all branches of a program will have been exercised significantly during the many operations by many different commercial customers. Additionally, because the development work is most often amortized across a broad base of customers, it can be less expensive. But the art of developing, applying, and certifying COTS software for safety critical systems is still immature. Therefore, the subcommittee asked for special assistance on this subject from John Stehnbit (R.E.&D. Advisory Committee member and new Chairman of the Committee), T.R.W. Corporation, and principally from Dr. George Allen, leader of the T.R.W. team that authored the expanded section on COTS at Appendix I.

Dr. Allen’s special appendix is an important review of problems associated with the use of COTS software. The members of the committee urge that the reader carefully study his entire treatise, which covers the following broad array of topics:

An initial discussion of the motivation for using COTS and the challenges this family of technology offers. This is followed by a review of the certification process in aviation, and a discussion of the approaches to COTS/Non-Development Items (NDI) in other organizations. The main portion of the report deals with COTS/NDI issues and their mitigation. From those issues and mitigation approaches flow the following set of recommendations which are noted here in a single overall recommendation format:

R-14: Recommendations from the COTS/NDI report:

A. The FAA should conduct an in-depth analysis of processes within the FAA which are affected by COTS/NDI technologies. This analysis should address the following:

1. Selection and engineering use guidelines.
2. Ideas for measuring and estimating the complexity of systems.
3. Develop a tailored life cycle model that addresses COTS/NDI components used in safety critical systems.
4. Develop a process to conduct preliminary risk assessments of systems that plan to use COTS/NDI.
5. Identify new methods to test and validate safety-critical systems which are not dependent on source code analysis.
6. Investigate ways to reduce the cost and time required to establish high confidence in a system.
7. Investigate ways to reduce cost and time required to re-establish high confidence in a system after a change is made.
8. Investigate ways to deal with interdependent properties and disciplines.
9. Explore domain specific architecture techniques to facilitate development and certification.
10. Develop new ideas to “fire-wall” functionality of COTS/NDI components within domain specific architectures.

11. Develop guidelines for use of NDI components acquired from domain-specific and general "re-use libraries".

12. Demonstrate the cost-effectiveness of the above techniques.

13. The FAA should analyze internal roles and responsibilities to include the following:

14. Investigate ways to involve critical functional elements of the FAA earlier in the system specification phase.

15. Assess modifications of the certification process and responsibilities to employ a "quick analysis" capability.

16. Identify ways to communicate to assurance and certification people.

17. Become a Beta test site for COTS products that are candidates for use in FAA domain specific architectures.

18. Promote software technology and process improvement techniques based on established best practice techniques.

19. Explore ways to expand current tracking of anomalies of COTS/NDI products by keeping statistics on product use throughout the computing industry.

SUMMARY OF SECTION II OF THE REPORT

The "Systems and Disciplines" section of the report deals with several specific technologies that are and will have a profound effect on the FAA and on AVR. Several areas such as the emphasis on simulation so fundamental to the "human factors" discipline, primarily augment the issues, conclusions, and recommendations outlined in Section I of the report.

The emphasis on "human factors", on simulation, on data warehousing for the complex information available from tests--incidents--and opinion surveys is warranted because of the accident statistics, that indicate the role of human error, or minor human deviations as causal factors in such a large number of accidents and incidents!

Many of the recommendations cannot and should not be implemented solely by AVR. They require additional research or development activity from the ARA organization, cooperation from other agencies, and an effective working relationship with industry. In particular, the entire discussion on COTS software, is more applicable to ARA than to AVR.

Two critical recommendations are aimed at improving the technical expertise within AVR and within the agency. The recommendation to hire more National Resource Specialists is vitally important. However, it is also critical to utilize these experts as the program originally intended. The FAA should ensure that they are able to hire the "very best" technical experts. These should be true specialists...not overly narrow, but certainly very focused in a specific technical discipline. Then it is also vital that they be utilized **as technical specialists not graduated into policy roles or other responsibilities that might dilute their ability to stay at the leading edge of technology and to advise broadly within the FAA on that field!**

USE OF COTS / NDI IN SAFETY-CRITICAL SYSTEMS

REPORT OF THE CHALLENGE 2000 SUBCOMMITTEE

of the

FAA Research, Engineering, and Development Advisory Committee

February 14, 1996

Contents

Executive Summary

The commitment to flight safety has prompted the FAA to ask the Advanced Technology Subcommittee of the FAA Research and Development Committee to review the current approach to certification of safety-critical systems in light of evolving technologies. The technology that is the focus of this report is the use of Commercial-Off-The-Shelf (COTS) and Non-Development-Item (NDI) hardware, firmware, and software components in computing systems. COTS/NDI technology also affects other systems under the FAA's purview, such as the National Airspace System (NAS), that require high reliability and assurance, therefore, the Subcommittee addressed the task with a broader view rather than focus only on safety-critical avionics systems. Although hardware, firmware, and software were evaluated, the report centers on software because it provides most of the functionality of computing systems and computing systems are central to avionics, and other FAA systems.

The Subcommittee evaluated the future direction of computing system development and software engineering; how other organizations are addressing the use of COTS/NDI in safety-related systems; the current certification process; and many of the issues and mitigation techniques related to use of COTS/NDI components. Recommendations were then formulated for consideration.

Safe and efficient air travel results only from a partnership between the FAA and aircraft operators. In its role as a regulatory authority, the FAA strives to work with the aircraft industry so the functional and economic benefits associated with new technologies are utilized in a timely way without jeopardizing safety. The integration of COTS/NDI components in safety-critical systems offers the potential to capitalize on technological advances by building computing systems which use computers faster, better, and cheaper. Like all technological advances, however, use of these products presents problems that are pervasive and annoying. We believe, however, they are manageable. The stakes are high; in safety-critical systems, a software failure can cost lives and destroy equipment worth millions of dollars.

The use of commercially available hardware and software components (COTS), or domain specific reusable software (NDI) is not just a trend, it is a sound architectural concept that is here to stay. Use of COTS is accelerating as the variety of COTS grows and the rapidly paced evolution of software engineering technology and techniques reduces reliance on totally custom-coded applications. The Subcommittee believes that the FAA and other Government agencies will have COTS/NDI components in safety-critical and other safety-related systems, and that current engineering practices and the FAA certification process require modification to address issues concerning the use of these components.

A continuing challenge for safety evaluation is not being able to test every combination of events in a large system. The test solution(s) are based on a systematic human analysis that determines those areas where the most testing or the most “over design” were required. In a sense, the objective has been to balance relative costs against risks in all parts of the system so that weak links were eliminated.

This approach continues today, but current circumstances highlight two weaknesses in the approach. First, today’s systems are much more complex than those even five years ago. This is true whether one measures complexity as the number of hardware components, number of lines of code in the software, number of software components, number of interfaces among components, or volume of data processed. As a result, it is no longer a valid assumption that a team of human analysts can adequately analyze the system in order to balance risks. It is far more likely in current systems that unanticipated interactions (rather than internal component "bugs") will underlie safety-critical failures of these systems. In short, yesterday's problem was that we couldn't test every combination of events. Today's (and tomorrow's) problem is that we can't even imagine some of the combinations that are critical to safety.

The second weakness concerns the tradeoffs between the cost of verification and the desired level of safety. The target levels of safety have, in the past, been driven largely by what humans could imagine. Humans could imagine a single plane crashing, and humans could (through systematic analysis) grasp the probabilities of failures that might lead to such consequences. There was an ability, as least in a qualitative way, to consider the balance between cost of additional verification/certification and the possible consequences of an error occurring. As stated above, the complexities of today's systems virtually preclude human understanding of the probability of safety-critical events. Simultaneously, the consequences of certain failures have risen to levels that are difficult for humans to balance against other criteria. What is the balance between the probability of a software bug and the consequence of meltdown in a nuclear reactor? What is the balance regarding an entire air traffic control network becoming inoperable with thousands of planes in the air? How many lives are endangered during an electric power failure that covers the entire northeast? Or by a telephone network failure that disrupts local or long distance communications? To make this assessment even more difficult, it is becoming increasingly important to consider the relative cost of not deploying a new system. If we fail to deploy a new air traffic control system soon, the probability of disaster appears very high. The need to assess the "cost of opportunity" was not nearly so important in the past when the environment surrounding a complex system was more stable. In today's world, the demands on existing systems are increasing very rapidly--so fast that the system must be upgraded just to maintain the status quo with respect to safety. For instance, the old air traffic control system is not merely degrading with age, the environment is changing. There is a much higher volume of aircraft than there was 10 years ago. If nothing is changed, the level of safety will not remain the same, it will plunge to unacceptably low levels.

This second weakness might be described as the lack of an explicit framework for balancing costs and risks. When the risk of retaining an existing system is variable over time, or when a new automated system is demonstrably less prone to error than the previous system (or the human operators that it replaced), then there is a real cost in delaying deployment. The Subcommittee recommends that the cost of delay be explicitly considered in all safety analyses.

The major Subcommittee recommendations are highlighted below:

1. Many of the COTS/NDI issues identified in Section 4 of this report relating to supportability, life cycle cost and engineering techniques have safety implications. The current certification process does not adequately address these issues as they relate to commercially available products or components acquired from reuse libraries and, therefore, should be modified.
2. Systems comprised of COTS components will be in a continual state of enhancement because of commercial market pressures levied on vendors to improve product functionality and performance. It is critical that the certification authority recognize that systems comprised of COTS products will be in a continuous state of re-certification throughout the life cycle. The certification process must be improved to offer early assurance that a proposed system is a good candidate for certification, and that the frequent system releases are certified in a timely manner.
3. A life cycle model that addresses use of COTS/NDI in safety-critical systems should be developed. The goal would be to balance the economic advantages, such as readily-available functionality at reduced cost, against safety-related concerns. New techniques should be identified for engineering disciplines such as requirement definition, test, safety engineering, and system validation and verification. At a

minimum, an early risk analysis should be employed to assess the safety of proposed designs. Extensive prototyping should be used to further investigate architectural alternatives and the applicability of candidate COTS/NDI components, and improved testing techniques should be applied early in the life cycle and continue until the system is decommissioned.

4. Develop a set of metrics to be used as a yardstick to measure system complexity as it relates to safety. The metrics would then be used to establish a threshold of system complexity that would ensure safety. Additional areas of analysis should include FAA domain engineering and architecture concepts, and associated reuse libraries.

5. An inter-agency “consortium” is recommended to develop consolidated selection and engineering use guidelines for COTS products, and to improve the Governments ability to leverage inter-agency collective requirements with vendors.

1. Introduction

It is impossible to overstate the importance the FAA places on the safety of the flying public. It is their commitment to safety that prompted them to task the Advanced Technology Subcommittee of the FAA Research and Development Committee to review the current approach to certification of safety-critical systems in light of evolving technologies. The technology that is the focus of this report is integration of Commercial-Off-The-Shelf (COTS) and Non-Development-Items (NDI) hardware and software components into aviation systems. Because the issues involving the use of COTS and NDI affect other FAA systems, such as the National Airspace System (NAS), the Subcommittee addressed the task with a broader view than explicitly avionics systems.

Although the Subcommittee considered the impact of COTS/NDI technical changes to hardware, the focus of the report is software. The reason for this is because hardware today is extremely reliable and expensive to change. Software, on the other hand, is more easily adaptable and it is where most of the system functionality resides.

Using COTS/NDI in these systems has specific implications for the safety certification process and general implications for the FAA's regulatory role. Since the issues with COTS products are pervasive throughout the computing industry, some approaches to mitigate issues are known and practiced. To solve the issues as they relate to safety-critical systems will require dedicating FAA resources to the problem, open dialog with the avionics manufacturers, and close coordination with the software industry. This report highlights many of the issues, provides possible mitigation techniques, addresses potential changes to the certification process, and recommends initiatives for the FAA to consider.

1.2 Approach

The Subcommittee assembled a group of technologists skilled in the software engineering and safety assurance disciplines to examine the certification of COTS/NDI in safety-critical systems. The group met on a number of occasions and "brainstormed" the topic. An extensive literature search, which included review of applicable government guidelines and regulations, provided research data that was complimented by "surfing the net" for additional information and points of contact. Experts in the FAA and other Government agencies, as well as industry experts, were contacted, in particular, those with expertise in software and those experienced in system safety.

1.3 The COTS / NDI Challenge

Computing systems are becoming more complex as more processes are automated to take advantage of the reliability and economic advantages offered by computing systems and as new concepts are developed to exploit the power of the computer. The functionality of the system is in the software which is not susceptible to the same deterministic analysis and testing as hardware. Software executes and performs as a function of variable inputs and its environment. It is flexible and adaptable to incorporation of additional functionality or performance improvements.

Furthermore, software engineering is a relatively young technology that is evolving at a rapid pace. Early software was monolithic and custom-crafted to the specific requirements of a particular system. However, the expense of software development and maintenance has forced innovative changes in the architectural design of software systems and in the way software is developed and maintained. Most important the computing industry has moved away from totally custom-developed systems. This movement began in the 1960's when multi-purpose operating systems were introduced and widely accepted. Commercially developed data base management systems soon followed and the trend toward integration of multi-purpose products into the infrastructure and applications of systems was born. The ever increasing pace of technology and intense computing has resulted in decreasing the time to market of innovative products and there is a seemingly insatiable appetite for new and better products. There is also increased automation of previously manual processes, and a widely accepted need to improve and integrate previously stove-pipe automated processes.

Users are reluctant to wait for a fully functional system to be developed using the traditional waterfall development life cycle model. A spiral life cycle model with incremental product deliveries appears to best satisfy the user needs and the trend to integrate COTS/NDI reusable components into system architectures.

Today’s market is dominated by architectures based on standards-based modular components, many of which are reusable. These reusable components may be Commercial-Off-The-Shelf (COTS) licensed software available from vendors, or previously developed domain specific Non-Development-Item (NDI) hardware, firmware, and software available as Government-Off-The-Shelf (GOTS) products. The move to open systems based on industry standards has encouraged competition and provides the buyer leverage in the market. In particular COTS vendors must build quality and performance into their COTS products.

Even if the FAA ignored this movement and insisted that safety-critical systems, or even the safety-critical functionality portion of systems, were developed using only custom-code that could be verified and certified using current in-place, proven processes, the time might come when this is no longer possible. The movement toward reliance on commercial software may result in a lack of individual skills and enabling technology to support custom-coded development of the scope and complexity required for ever more demanding requirements. The FAA has no choice but to have systems that have COTS products integrated into their architecture and the well being of thousands of people will be dependent upon the reliability, integrity, safety and security of these systems.

The role of the software engineer is changing. The trend is for computer programmers to be employed by commercial vendors, such as MicroSoft and Oracle, rather than application development organizations, such as Government contractors. Technological advances in software development tools and process automation are making a dramatic impact on computer programming. As these technology changes continue, systems will increasingly be built by a new breed of system engineers and only unique, application-specific components will be custom-coded by computer programmers. In this scenario, software development activities are performed under the direction of domain engineers in close coordination with end-users, or by end-users themselves, using an

Integrated Software Engineering Environment (I-SEE) toolset. In effect, domain engineers "own" the business process, while end-users are the primary source of recommendations for improving the supporting information systems. Code will originate from three sources: (1.) it will be automatically generated via the I-SEE environment, (2.) it will be obtained from domain-specific reuse libraries or from COTS/NDI commercial products, (3.) unique, specialized components will be custom-coded -- in ever-decreasing quantities as more reusable components become available. The developed system will be comprised of integrated software components derived from these three sources.

A primary challenge facing the Federal Aviation Administration (FAA), and other Government organizations, is to continue to carry out the mission of providing safe air travel to the public at a time of constrained funding levels. The significant economic advantages of using COTS components in computing intensive systems include decreased system development time, cost-sharing of the component development by a large market, and extensive testing by a large, diverse user base that will result in safer software. NDI offers the same economic advantages, but testing, though thorough, is performed by a focused community of users. Accompanying these advantages are technical and administrative challenges for systems using COTS and NDI. These challenges are heightened for safety-critical systems, such as air traffic control, avionics, nuclear power, medical, and space exploration where human life is endangered if system errors are encountered. Many of the issues involving use of COTS/NDI and possible mitigation techniques are identified in Section 4 of this document.

1.4 Motivation For Using COTS/NDI

There are clear motivations for using COTS or NDI components to produce complex FAA software systems:

- Time to deploy: system needs dictate more rapid development of capabilities
- Economic: the non-recurring development cost, extensive testing, and most of the maintenance expense is spread over the entire customer base of the product

- Identified defects: there is a large, diverse user base for error discovery
- Competition: market pressure motivates the vendor to deliver quality software
- Increased complexity: Users are requesting additional functionality which results in additional complexity.

Building systems of distinct components that are glued together via recognized standards is widely accepted in the industry today. A standards-based open system architecture provides a framework for integration of components, which may include COTS/NDI products. Open systems standards provide common rules, guidelines and characteristics that support component integration. The economic incentive for COTS vendors to develop products that comply with open systems standards is that more copies of the product may be used because of its' ease of integration. Standards also ensure "similar usage" across many diverse systems and result in fewer bugs in these standards-based systems. The incentives for designing a component-based open systems architecture are that the system will offer portability across platform types, afford interoperability with other systems, will provide scalability of applications and data, and will increase competitive pressures on vendors to deliver less expensive, quality products.

The demands of market competition to deliver faster, better products motivates commercial vendors to hire the best and brightest software engineers who are drawn to vendors because of higher salaries and challenging work. This is in contrast to the recent past when the aerospace industry was the premier employer of the best software development talent from the best universities. The FAA can capitalize on this trend and the competitive drive of vendors to deliver products better than the competition through the use of COTS products; it is truly a buyers market.

There are significant economic advantages to the use of COTS products when developing systems. Windows95, for example, consists of approximately 2 million lines of code and costs $90. The non-recurring development costs are shared over the entire customer base of the product, thereby reducing the cost to each user. The cost to fix latent errors and implement enhancements is also shared by the customer base throughout the life of the product. The most significant economic advantage, however, is the ability to develop systems faster because so much of the needed capability is available in commercial components. The need to develop systems faster is driven by the rapid changes in technologies that the application may be dependent upon.

Development risks and schedules for systems may be reduced by including the readily available technical capabilities offered by COTS/NDI components. One or more components can frequently be evaluated in a prototype of the system before a commitment to purchase the product is formalized. Vendors are anxious to prove the benefits of using their product.

The advantage of using products with a large, diverse user base cannot be overstated. COTS products are generally better tested through this large user base than components that were custom-coded for a particular system. Conventional methods of testing a system with a given set of test scenarios cannot begin to cover the depth and breadth of testing by a wide assortment of users employing the product in many different application types. In a safety-critical application, however, it is important to ensure that testing of the system is not curtailed due to reliance on product testing of this wide user base.

2. Certification Process

Traditionally, airworthiness certification relied on extensive reviews, which were facilitated by stringent documentation requirements. From the beginning of the engineering process, the component was intended for use in a safety-critical environment and the manufacturer worked with the FAA to ensure the opportunity for reviews and for timely addressing of any concerns.

For reasons described above, there are many benefits to being able to use COTS equipment that was not originally intended for use in safety-critical systems, although built with rigorous quality standards. The FAA has begun addressing the adaptation of Certification standards to be able to address issues such as the “reuse” of various hardware and software components and integration of the proposed new installation with existing or other planned systems onboard an aircraft.

Current airworthiness certification procedures rely on an interactive process between the FAA and the applicant for design approval. In the past, the FAA has relied on RTCA, Inc. as a forum for establishing Minimum Operational Performance Standards, which provide an opportunity for coordination between the rule-makers and industry.

There are three ways that an avionics system may be certified — by Type Certificate, Supplemental Type Certificate, or Technical Standard Order:

- The system may be part of a new or modified airplane design produced by an airframe manufacturer. In this case, the system certification would be covered under an aircraft Type Certificate (TC).
- The system may be added to an existing airplane by an organization other than the airframe manufacturer (TC holder). In this case, the system certification would be covered by a Supplemental Type Certificate (STC).
- The system may be certified independent of the aircraft on which it is to be installed. In this case, the system certification would be covered under a Technical Standard Order (TSO). Installation of a TSO’d system on an aircraft will normally require a TC or STC.

Systems and equipment to be installed on transport category aircraft must meet the requirements of Federal Aviation Regulation (FAR) 25.1309* . Advisory Circular 25.1309-1A describes acceptable means of compliance with FAR 25.1309. This circular addresses the requirements that:

- "The equipment, systems, and installations … must be designed to ensure that they perform their intended functions …"
- "The airplane systems and components, considered separately and in relation to other systems, must be designed so that:

1. The occurrence of any failure condition that would prevent the continued safe flight and landing of the airplane is extremely improbable, and
2. The occurrence of any other failure conditions which would reduce the capability of the crew to cope with adverse operating conditions is improbable.

- Warning information must be provided to alert the crew … and to enable them to take appropriate corrective action. Systems … must be designed to minimize crew errors which would create additional hazards."

Certification procedures are already in the process of being modernized. The most important aspect is failure analysis; how bad is the impact if the component fails to perform as expected? The emphasis is also shifting to having the applicant take most of the responsibility for determining the approach. This is particularly valuable since the applicant will have been involved in determining that the proposed component is suitable. Because of the applicant's familiarity with the system and the COTS product's role within the system, it should be possible to determine a mechanism for verifying and validating the suitability of the equipment for the application. The applicant's analysis should include evaluation of all possible ways in which the product can contribute to a system hazard. The FAA's cognizant Aircraft Certification Office (ACO) must be involved early to ensure that the processes are adequate. To some extent, this would be akin to an ISO 9000 certification, in which an applicant must

* General Aviation Airplanes are covered by FAR 23.1309 and Rotorcraft are covered by 27.1309.

prove that it has adequate quality procedures but the certifying authority does not dictate those procedures.

Efforts are already underway to use better, more efficient ways to process and achieve certification approval, as long as traceability and credibility in context are preserved.

When COTS software is used, because monitoring of development processes may be difficult, software quality assurance (SQA) and Configuration Management (CM) procedures are particularly important. Documentation must include a description of interfaces, control and data flow, partitioning, and error detection. It's accuracy and completeness should be evaluated.

In the failure effects approach, it is necessary to show by the system architecture that the COTS component could not contribute to a critical failure. Any installed part must contribute to integrity. A concern that must be address during certification is the possibility that the COTS component may behave in unanticipated ways, or interact with other components in unanticipated ways, that do not violate their specifications. One advantage of COTS with respect to certification is that there may be far more service history data available than is true with customized components. Service history data may be used if it can be shown to be applicable and that any changes between the history environment and the proposed environment can be rationalized.

The FAA has already begun to address the issues of certifying systems that rely on the use of commercial hardware or software products as part of its process for planning for the use of Aeronautical Data Link. The approaches documented in “Guidelines for Design Approval of Aircraft Data Communication Systems,” Advisory Circular 20-DC should be expanded and used as the basis for a revision of FAA Advisory Circular 25.1309.

Because certification procedures affect aircraft flying international routes, and aircraft operated by non-U.S. carriers, it is mandatory to harmonize any changes to airworthiness certification procedures through the International Coordination Panel for Navigation and Communication.

3. Approach To COTS / NDI In Other Organizations

COTS components are currently used in the software infrastructure and hardware microcode of many safety-critical or safety-related systems. The topic of certification of safety-critical systems, and validation of general purpose systems that contain COTS / NDI products is not unique to the FAA. Other governments, various U.S. Government agencies, commercial companies, industry consortiums and standards bodies are addressing COTS / NDI challenges similar to the FAA. The Subcommittee informally surveyed the computing systems community to identify related activities, some of which are summarized below.

3.1 Experience In Other Organizations

The Department of Defense (DoD) has many systems that are safety-critical in nature and relies on Mil-Std-882C, *System Safety Program Requirements,* for guidance. The Tomahawk Nuclear Vertical Launch System, which used a Unisys COTS operating system, followed the guidance provided in Mil-Std-882C when developing the system safety program. During the hazard analysis of system components it was decided that the Unisys COTS operating system was of such a critical nature to the system that the source code had to be verified by an Independent Verification and Validation (IV&V) contractor before certification.

NASA is integrating COTS software components into NASA's Space Station Program. The well being of the astronauts who utilize this system will be dependent on the reliability and safety of these integrated component based systems. NASA plans to perform white box testing, a strategy that derives test data from knowledge of the program's internal structure, of this safety-critical system.

Duke Power uses IBM RS / 6000 workstations with AIX operating system in nuclear power plants to perform safety-related functionality. They also use Excel spreadsheet that have been integrated into a system to calculate data used for visual displays (temperature, pressure, etc.) in power plants in applications the Nuclear Regulatory Commission (NRC) considers Important to Safety Functions. The COTS / NDI components are tested in the context of the total system under safety program defined procedures. Duke Power representatives view the wide commercial use of COTS/NDI products as added assurance of the viability of the components integrated into their systems.

Amtrak railroad has integrated commercial hardware products into their system for many years and has extended their use of commercial products to software. Major companies provide products in signals, electrical substations, communications, track, platforms, tunnels, etc. Application of a program similar to MIL-STD-882 was used in the specification requirement by the Amtrak railroad system to assure that designers had a solid system safety program in place. No contract was signed without the requirement for a *System Safety Program Plan* and later the *System Safety Hazard Analysis* which the designers performed. Design reviews were conducted with the contractor designers providing the hazard data for their infrastructure area. The Federal Railroad Agency (FRA) performed auditing of this program to assure that safety was evident in all required areas. Hardware as well as software was examined as a part of the total program development.

Although COTS/NDI components are increasingly being integrated into systems, there is no consistent approach to selection and use of these products. COTS is used with and without source code evaluation, white and black box testing techniques are employed, but the amount of testing appears to vary. Other organizations are faced with the challenge of how to verify COTS/NDI products.

3.2 Development Of Standards And Guidelines

The National Institute of Standards and Technology (NIST) is developing guidelines for programs to use when using COTS/NDI components in systems. This work is being done for the health care industry, which requires high assurance software.

The U.S. Air Force has provided guidance for selection and use of COTS products in their *Guidelines for Successful Acquisition and Management of*

Software Intensive Systems, available from the Software Technology Support Center, Hill Air Force Base, Utah.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are jointly developing an international standard for qualifying off-the-shelf products for safety-critical and safety related applications. A working draft is currently published for review.

The, Dr. Floyd Hollister, FAA Chief Scientist for Software Engineering (AIT-5) has an on-going task to address the subject of COTS/NDI products integrated into FAA systems. Current work includes development of a *Program Manager's Guide to COTS/NDI Software Use in The FAA* which will be followed by an implementation guide.

4. COTS / NDI Issues And Mitigation

There are many issues that are important for the FAA to consider when designing and building systems that contain COTS / NDI components. As the task assigned to the Subcommittee was to evaluate the impact of COTS / NDI technology on safety certification, the impact of all identified issues were considered before recommendations were made. The following are some of the most important issues identified, coupled with possible mitigation techniques. The issues are grouped into two categories:

- Technical.
- Management.

4.1 Technical

This section discusses the technical challenges associated with COTS integration that are considerations for evaluation of safety-critical systems.

4.1.1 Complexity

Issue: In data provided by Dr. Edwin Stear, COTS was used in the Boeing 777 for such things as cabin environment control, ice protection, communication, the brake system, and warning electronics. COTS was also used as computing infrastructure support for a bridge router and cabin file server. There is surely interaction between many of these capabilities leading to a complex array of functionality.

Users throughout the computing industry are demanding that more and more functionality be automated and they are no longer satisfied with stove-pipe systems. They also want their systems to be user friendly with graphical interfaces, windowing, pull-down menus, and to be able to point and click to a wide range of capabilities. Legacy systems are being migrated to higher performance hardware and users frequently want to augment existing systems with a wide range of desk-top capabilities.

This insatiable appetite for increased automation is causing computing systems to become highly complex. This complexity falls into two categories:

- The sheer volume of computing states
- The complexity of algorithmic control structures.

A key cause of failure within computing systems is the unexpected concatenation of unusual states in independent parts of the system, i.e., status indicators that are invalid causing unintended computing activity. The likelihood of this happening increases as functionality is added because the number of possible states in a system increases and, consequently, the complexity of control structures multiplies. When Artificial Intelligence (AI) techniques are used, predicting the states of the system using traditional hazard analysis techniques becomes even more difficult, if not impossible.

COTS software is growing increasingly complex as each vendor includes more and more functionality in order to broaden the market base. Some features in a product are unneeded in a specific system, or, worse yet, potentially harmful because of bugs or unspecified and unwanted interactions. The problem gets worse as the number of COTS components are integrated into the system architecture. The complexity of COTS components is difficult to assess because:

- There is little or no insight into the internals of the product
- The product contains functionality that is not planned to be used by the system
- The anomalous interaction between COTS components is difficult to predict
- It is difficult to anticipate the consequences of modification.

An increasing number of systems are distributed dynamically across a heterogeneous network of computing resources. And “wrapping” legacy code using Object Request Brokers (ORBs) to facilitate distributed computing is becoming increasing common. Establishing the correctness of such systems is much harder than in a static single-processor environment.

Human system developers and integrators cannot hope to keep pace with this increased complexity unless techniques and tools are developed to reduce the apparent complexity of systems. Advanced methods are required to reformulate the safety-critical system development process.

Mitigation: There are approaches to manage complexity. A critical first step is to develop a standard yardstick for safety. The absence of such standard measures, however informal, limits research in the area. Clearly a metric, or set of metrics, to quantify the balance between safety and system complexity should be identified. The threshold for this metric should be identified early in the requirements specification phase and be the determining factor for the complexity of the system being developed. The System Safety Requirement discussion in Section 4.2.4 presents the concept of "design to safety" in which this metric is a defining factor in system requirements. We need explicit safety metrics, objectives, measures, etc. At a minimum, the metrics would be used to determine via prototyping if system A is safer than system B.

Secondly, the FAA should develop rules for avoiding complexity. A mechanism to implement the rules is to identify, and classify reusable architectural templates designed to reduce complexity and partition COTS components within the architectural framework to contain errors. The following section, Architecture and System Engineering, proposes such a concept.

The third step is to promote analysis in the theories and tools that help in measuring and developing safety-critical systems. Many of the same techniques that make software systems more understandable to humans will also make it more feasible for automated program analysis tools to deal with complex systems and, for example, to verify that a COTS component meets certain safety criteria.

4.1.2 Architecture And System Engineering

Issue: In the past, safety-critical systems have failed because of incorrect or incomplete specifications, lack of full understanding of the implications of requirements changes, and unforeseen dependencies or interactions among elements of the system. These failures usually trace back to inadequacies in system architecture and system engineering, as opposed to the software employed in system implementation. Yet the use of COTS components has implications, both positive and negative, for dealing with such failure mechanisms.

Prior to the 1980's, system architects used redundant mainframe and mini hardware, together with tightly managed, highly structured software to build safe systems. Once powerful microprocessors became available, system architects began employing federated systems, i.e., they have partitioned the system into functionally independent subsystems, each providing minimal functionality or services. The idea is to prevent the propagation of errors from one subsystem to another and to be able to isolate errors easily while having high confidence in each module. Such systems may even use separate hardware to host the subsystems to further reduce the possibility of catastrophic failure. In the past, such an approach was expensive and very demanding of both management and system engineering talent, since the allocation of function and coordination of many separate developments was essential to success.

Today, the trends in the commercial market give promise of reducing costs and empowering management and system engineering. The infrastructure components of commercial distributed systems are candidates to support safety-critical federated architectures of variants structured to exploit COTS. One can envision an implementation of federated microprocessors using COTS hardware, operating system, communications software, and middleware to exploit commercial trends while building a sage system. Such an implementation provides redundancy and the potential for fault tolerance. (Although the availability of COTS was limited at the time, this was the approach taken on AAS).

Unfortunately, such distributed systems are inherently more complex than single-node mainframe systems and more likely to exhibit unanticipated, and possibly unsafe, behavior. It is more difficult to identify the causes of hazards (possibly even the hazards themselves) if the causal system is distributed. And yet, since the availability of applicable COTS is market driven, it follows that the move to distributed systems in the commercial market will exert pressure to use distributed architectures in safety-critical systems in order to exploit COTS. Furthermore, the skill base for implementation of architectures other than those promoted commercially is likely to erode over time, making such an architectural choice less attractive.

However, commercial vendors are being driven by market forces other than safety, though reliability, an important component of safety, is generally a market driver. Vendors are addressing the market with system architectures and technology that do not provide immediately applicable COTS products for every safety-critical system requirement. The use of COTS is analogous to “design to cost” in that the system may no longer be specified or functions allocated optimally. Rather, compromises are made to exploit existing (or planned) COTS. It is important to identify the compromises and analyze them for safety implications. Still, the appeal of COTS for all but the special applications needs of a safety-critical system is undeniable in terms of cost savings, time to deployment, and the inherent reliability in appropriately selected, widely-used COTS products.

Mitigation: Steps to approach this problem are:

Certify Domain Specific Software Architectures (DSSA) for Safety-Critical Systems.

It is feasible to develop and certify complete architectures or architecture components for ATC, avionics, surveillance, etc. Manufacturers or FAA contractors would then use these architectures and add application code or glue code only. The artifacts would then become candidates for inclusion into the FAA reuse library as NDI assets. The advantage is the greater usage and consequent improved reliability of the components or the architectures and the increased talent pool available to implement the constrained set of architectures. This approach has been investigated by The Advanced Research Projects Agency (ARPA) and is being implemented by DISA for U.S. Army C3 systems.

Use the DSSA to Constrain the Use of COTS.

The suitability of a COTS product is partly a function of the DSSA. For example, in a single-processor system or one with minimal communication among nodes, the network manager is either unnecessary or minimal in function and its impact on system performance. Hence, it should be relatively easy to ensure that any network manager, COTS or not, will not affect safety. However, in a distributed system with many interacting nodes, the network manager becomes a key to system performance which, in turn, could impact system safety, leading to the usual tradeoffs regarding COTS vs. developed software.

Once DSSAs are established and certified, the role of individual COTS products in each DSSA will be determined and there will be different constraints on the use of COTS, depending on the DSSA as well as the characteristics and history of the COTS product. For example, the constraints on application code in a DSSA that permits no direct interfaces to other applications will be different from that on an operating system which could interface with and impact many different code modules.

Use COTS Components That Have Been Extensively Stressed.

Clearly, one of the qualifying conditions for using a COTS product is that is has been used extensively and is thus thoroughly tested and reliable. However, for COTS products that are critical to safety (Level A, B, or C), the constraints could be more restrictive. For example, given the complexity of the telephone system, financial systems, and many DoD systems, one could insist on extensive and successful usage in such systems. It should also be possible to collect relevant data on product performance and anomalies from system managers. The key is to select

COTS products that have been stressed in application environments that are sufficiently demanding that they are likely to uncover software errors that could impact safety.

It is a consequence of this selection criterion that the selected COTS products should only be used within the mainstream of their previous employment. That is, the product should not be employed in a manner that attempts to exploit little-used features or that demands performance beyond that required in previous applications of the product. In particular, the tiering of COTS products, embedding one within the other, falls within this constraint.

The advantages accrued in product selection following the guidelines suggested above will likely be lost if the COTS product is modified by the system developer. Modification of COTS products should be forbidden unless the vendor makes the modification, agrees to support the modification in future releases, and tests the modification to the satisfaction of the buyer. Even under these circumstances, modification should be discouraged, since the advantages of prior extensive product use are foregone. Minor tailoring of a product, e.g. to eliminate unwanted functions, is permissible as long as the tailoring is within the guidelines provided by the vendor and will not affect vendor support.

The move to open systems in the commercial market can also be exploited, though the requirement for open solutions can be undercut by the competing organizations pushing their brand of openness. The real advantage is that the drive toward open solutions has increased competition and forced vendors to improve the quality of their product, an important component of safety.

Test Alternative System Infrastructures.

Though industry experience is still limited, the most serious problems with distributed systems and those most difficult to identify and fix are those associated with the infrastructure, not the application code.

Fortunately, given the commercial tools available, it is feasible to postulate, build, and test alternative architectures prior to committing to a design. This is ordinarily done to ensure that the selected architecture meets the performance requirements. However, the alternatives could also be compared with regard to safety, e.g. by testing and comparing for environmental robustness, tolerance to out-of-spec inputs, or recovery from failure.

The alternatives should also be compared for ease of technology or new product insertion. An architecture that truly supports “plug and play” is more amenable to absorbing the requirements changes that are common in software-intensive systems and is inherently safer than one that requires extensive modifications to accommodate change. A related issue is the need to deal with version upgrades that may be inconvenient or downright disruptive. The ease with which an architecture can deal with such disruptions should be a major criterion in selection.

Test Alternatives in the Target Environment.

While it is wise to select COTS products that have been used in stressful environments, it is unlikely that products can be found that have been used in the same environment with the same set of COTS products required for the target system. It is essential that the investment be made to test alternatives in the target environment before an architecture is selected. Experience shows that this is the only way to discover interface incompatibilities and other unforeseen interactions that are specific to the target environment (see Section 4.3, Integration Issues). Claimed capabilities and performance must be demonstrated.

4.1.3 Security

Issue: System security may be compromised by any malicious individual, but introducing products with un-verified product assurance manufacturing practices increases the possibility of a breech in security. There have been well publicized cases where security was compromised by the introduction of a virus or a Trojan horse capability into the system, or by malicious conduct by an individual.

Evaluated COTS security (trusted) products, e.g., operating systems, data base management systems, network products, are available; however, incompatibility between vendors remains a major obstacle for an integrated solution. Maintenance of security and safety assurance is also a primary consideration in COTS/NDI use decisions.

Mitigation: In addition to determining the assurance criteria that is acceptable for each system component, guidelines should be developed that detail the selection criteria for COTS/NDI components. System security must be addressed throughout the system life cycle beginning with strategic planning. Architectures and designs can provide such safety/security approaches as separation kernels and reference monitors to permit selective COTS/NDI use.

4.1.4 Life Cycle Changes

The integration of COTS/NDI components into a system necessitate life cycle changes. When they are to be integrated into a safety-critical system, there are additional considerations that require life cycle modifications.

Integrating COTS packages in a safety-critical system involves trades to achieve an optimal design solution, given the issues and concerns presented above. It is clear that there are no universal guidelines when considering using COTS in safety-critical systems. Rather, disciplined specification, design, development, test, and analysis processes aimed at avoidance, discovery, and containment of failures should be employed. Specifications aimed at minimizing outages by addressing a system as a provider of services and adopting a service outage perspective, including explicit definitions of service attributes and criteria to determine service outage, should be considered. Design strategies based on functional redundancy and defense-in-depth, such as the use of design/architecture hierarchies with well defined service attributes for each hierarchy, should also be considered. Analysis techniques such as Failure Mode Effects and

Criticality Analysis (FMECA) and Fault Tree Analysis (FTA) should be used to identify potential design weaknesses and support the development of failure mitigation tactics. Aggressive test programs that prove the system's compliance with requirements in fault free and faulty environments (through fault injection) should be used to maximize failure discovery rate during testing. Finally, the use of techniques such as assertion checks and acceptance testing to validate the inputs and outputs of the COTS component should also be considered to improve the system's failure detection capability.

The unique problems associated with COTS integration necessitate in-depth evaluation of the acquisition life cycle. The following sections discuss the most important considerations to be addressed when COTS / NDI is planned for safety-critical systems.

4.1.4.1 System Safety Requirements

Issue: Simplicity is one of the most desired attributes in a safety-critical system. Today, system complexity, as opposed to simplicity, is a major concern in safety-critical systems. The system specification (A-Spec), based on the intended concept of operations and the perceived needs to be satisfied by a system, is a major determinant of the eventual simplicity or complexity of a system (the system architecture and design are others).

The prevalent approach to writing a system specification is to convene a system engineering team with representatives from all affected parties, e.g. architects, system engineers, users, technical specialists, trainers, maintainers. The intent is to find a compromise between desired capabilities and available cost and schedule. Best architecture and design practice then emphasizes ensuring the fielded system can be easily modified to accommodate new technology, new products, new functions, and improved performance. Thus, the compromises made at the time of initial specification hopefully become temporary, with the expectation that all communities will be more fully satisfied in the future.

In such a specification environment, with the future uncertain, there is a strong tendency to try to satisfy the various constituencies in the initial specification or in the modifications introduced during an incremental acquisition. This often leads to systems that are, perhaps, over-specified in terms of performance and function compared to the bare minimum capability needed to fulfill the operational need. In today's environment of computational and communications largess, this tendency has become more pronounced. Furthermore, the understandable concern with the human user's ability to cope with the growing complexity of systems (and possibly the environment) has further motivated the desire to introduce more automation, e.g. knowledge-based systems. While this can aid the user, it complicates the system even more. Free flight and collision avoidance are examples of this trend.

Mitigation: A more appropriate approach is a modification of the "design to cost" model - a "design to safety" concept in which the goal of simplicity, as opposed to function, performance, schedule, or cost becomes paramount. In effect, a new constraint on complexity (like permissible cost or schedule) would be given the A-Spec team. Function and performance would be limited or traded off (if necessary) with additional complexity which could affect system safety. This approach would be followed throughout the architecture, design, implementation cycle.

Such an approach requires measures of system complexity, i.e., metrics, applicable to all phases of system conceptualization and implementation. It would be particularly convenient and effective to have metrics applicable early on during specification, since the cost of changes or correction ordinarily increases during the implementation cycle. However, the implications for system complexity may not be evident during specification. Hence, it is particularly critical to formulate metrics for comparing alternative architectures and designs for complexity. It is even better if these metrics can be augmented with comparative data derived from building and exercising models or prototypes of alternatives.

Unfortunately, there are no generally accepted metrics of system complexity, although most practitioners would agree on some rules of thumb related to the stringency of the performance and reliability requirements, or the number of nodes and users in the system, for example. There is also no generally accepted metric for software complexity for the large, high-performance, real-time systems embedded or otherwise, which are characteristic of FAA's safety-critical applications. Thus, today's practitioner uses combinations of (usually inadequate) metrics, rules of thumb, experience, intuition, and combinations of modeling and prototyping to predict the ultimate complexity of fielded systems.

The above discussion is independent of the use of COTS, but the use of COTS has implications for the discussion. For example, from a positive standpoint, the existence of COTS provides a realistic basis for specification, i.e., users tend to accept what is available and familiar and be less insistent on "nice to haves". Also, COTS can be integrated into an architectural prototype early on and tested to provide greater assurance of system safety. In general, even though there may be integration or other problems later, the reduction in the number of unknowns by using COTS is positive.

4.1.4.2 Early Risk Assessment

Issue: Many of the risks associated with COTS/NDI have only recently been identified and standard practices for assessing and mitigating them have not yet been developed. Integration of COTS into safety-critical systems poses additional risks. Development projects are sometimes well into the life cycle before problems are recognized resulting in delays or unanticipated costs.

Mitigation: An assessment of risk associated with integration of COTS/NDI into a safety-critical system should be performed early in the life cycle. A cost/benefit analysis should be conducted to determine the impact of the management issues raised in Section 4.1. A primary objective of the risk assessment should be to determine the likelihood of the proposed alternatives meeting safety-critical requirements. The risk assessment should evaluate if the additional cost of COTS-inspired safety enhancements negate the cost benefits of using COTS products.

The certification process should be modified to employ a quick analysis methodology early in the system life cycle to address the acceptability of the solution of the system under consideration. This approach offers the advantage of identifying, early-on, potential design, cost, or supportability issues that may jeopardize safety.

4.1.4.3 Prototyping

Issue: Prototyping is a common technique used to assess the viability of a design concept. It is also a good mechanism to evaluate the appropriateness of a particular product within the architecture. Design decisions are frequently based on the low-cost alternative of integration of an available commercial product into the design. The appropriateness of the COTS/NDI product to the safety requirements of the system must be assessed.

The low cost option of decreased development and rapid deployment leaves the system exposed to defects in the COTS/NDI component itself or to new defects due to the package's behavior within the system. The alternative of developing custom software according to safety-critical software development standards is expensive and time consuming. It is unlikely that the COTS vendor will enhance or modify their product to overcome perceived system vulnerabilities introduced by the commercial component. Additionally, the use of multiple COTS components increases the complexity of the system which increases the vulnerability to error.

Mitigation: Prototyping provides a way to quickly represent customer requirements in a limited way throughout the integration life cycle. Use of prototyping assists communication between the domain engineer, or system developer, and the user of the system. It is a proactive technique that will support safety assessment of the system because it focuses on thorough understanding of requirements. Development and execution of prototypes provides a way to address problems of ambiguity, incompleteness, and inconsistency in capturing the requirements of a complex computing system.

The decision to use COTS components in a safety-critical system architecture must weigh possible increases in system vulnerability to hazards or failures against potential cost savings attributed to decreased development activity and rapid system deployment. In addition to this trade-off analysis, and prototypes of architectural design options to contain adverse effects of failures attributable to the COTS/NDI component should be considered.

First, the FAA should approach the vendor to determine if the vendor would modify the COTS component to meet derived safety-critical requirements, or explore the ramifications of modification of a NDI component. The shortcomings of this approach are both technical and economic. Technical issues include the difficulty in establishing the appropriate level of "robustness" for the package as well as assessing this robustness within the system. Economic issues include the vendor's reluctance to commit funds to provide a robust COTS component because of the limited market for this product type; the FAA may have to fund the vendor's activity, but then to what level?

The option of designing constraints within the system to contain the adverse effects of failures attributable to the COTS/NDI component is more promising; it focuses system development on the key issue of the behavior of the component within the system architecture. This option requires some level of design and/or development to implement the desired level of protection that can be economically evaluated through prototyping. All containment approaches involve the use of software "fire walls" to shield the component within the system architecture and validate its inputs and outputs. The notions of "validating" the COTS component inputs, such as using assertion checks, to ensure their compliance with the input specifications and performing "Acceptance Tests" on the component's output parameters to ensure their compliance with its output specifications are techniques for improving the system's ability to detect COTS failures. However, this option does not eliminate the vulnerability to COTS defects, it merely allows for additional protection against failures. Moreover, the additional code needed to implement the assertion checks and acceptance tests may also be a source of errors itself unless its size and complexity are well managed. Finally, system performance is adversely impacted because of the overhead due to executing the checks. Prototyping will give insight into the severity of performance degradation.

4.1.4.4 System Integration

Issue: Industry experience with COTS provides ample evidence of the difficulties encountered in the integration of COTS products. Each combination of products and each computing environment presents unique problems. The causes are varied: incompatibilities, incomplete specifications or interfaces that do not perform as specified, software bugs, inadequate hardware, product performance degradation in certain configurations, and so on. Even if the selected COTS products are fully compatible and work as advertised, it may be that the system integrator is inexperienced in the use of the components. In this case, the product may be misused or not fully exploited

Mitigation: The consequence is that it is not feasible to select a total system configuration using COTS, until the products have been integrated and tested together as a system in the target environment by knowledgeable people. Otherwise, the potential for change and schedule impact is considerable.

There are no shortcuts - an investment in equipment, products, tools, prototyping and training is a prerequisite for successful employment of COTS products in any system, more so in one in which safety is a requirement.

New features of COTS/NDI components are sometimes difficult to integrate. Vendors over-promise capabilities and ease of use of COTS products, and NDI components functionality may not be completely understood. Side affects from integrating software products not designed to go together, or product features available but not used, is an additional concern, especially under stressed operational conditions.

4.1.4.5 Test

Issue: Unfortunately, there is no timely way to test a system specified to have high reliability, so as to have high confidence that the system does, in fact, meet the specifications. This was reported in a NASA Langley Research Center report by R. W. Butler and G.B. Finelli titled "The Infeasibility of Quantifying the Reliability of Life-Critical Real-Time Software". There will be errors in delivered systems, safety-critical or not. Some of the errors will have implications for safety. The most insidious errors are those with a very low probability of occurrence (so-called 5000 year errors), but with the potential for deadly consequences if they occur. Not too surprisingly, 5000 year errors make up a substantial proportion of the latent errors in delivered software, about one-third in a product sampling done by Bev Littlewood and Lorenzo Strigini at IBM Research and reported in the *Scientific American*, November 1992 article titled "The Risks of Software". They are the errors least likely to be found during standard product testing.

If one assumes there is one error for every 1000 lines of delivered code, a COTS product with 3,000,000 lines of code (e.g. Windows 95 or AIX) will contain 3000 errors, about 1000 of which are 5000 year errors. Over a 20 year system life, the likelihood of occurrence of a 5000 year error is about .98, considerably less in a single user's system, depending on the nature of the bug and the stressfulness of the application. Even if only 10% of the 5000 year errors are critical to safety, the probability of an occurrence in some user's system is about .33. Even if this is overstated by an order of magnitude for a given user, it is still troublesome. The chance of finding the bug and correcting it before damage is done is directly related to the amount of testing and usage the software receives, assuming the testing and usage fully stresses the software.

Compared to the usage of a popular COTS program, very few people exercise a unique safety-critical system over its life. A unique safety-critical system running 24 hours a day for 20 years accumulates about 175,000 hours of usage over its lifetime. This is a trifle compared to a COTS program used by 20,000,000 people for 4 hours a day, on the average, for its life of 3 years, say. The usage will total about 80,000,000,000 hours or over 450,000 times as much as the usage of the safety-critical system, increasing accordingly the opportunity for error discovery.

When developing systems that contain COTS components, error detection and resolution requires special consideration. There may be no visibility into the internals of the component, or the functionality of the software may not be fully utilized, or the software may be uniquely implemented. Errors may be the result of integration with legacy code. Additionally, errors may be introduced into the system by tools, such as compilers, used to support the software development process. The result is that the system presents complexities that are difficult to assessed.

An internal fault may be due to a design or integration fault of the COTS component itself. Indeed, the possibility for this type of source of errors continues to increase because of the growth in capability and complexity as well as size of COTS components. Causes of the fault rate are numerous; they are primarily driven by short development schedule pressures due to market competition and quality control processes that, while consistent with the target applications of the software, may not be consistent with software to be used in safety-critical applications.

Mitigation: The approach to testing is straightforward, if arduous and expensive. Begin testing as soon as possible and never stop during the life of the system. In particular for distributed systems, first develop and test the architectural infrastructure before integrating any application code (see Section 4.2). Search diligently for weaknesses in the architecture, design, and implementation by stressing the system beyond its specified limits and determining its break points. Use “bonded hackers” to try and infiltrate and break the system. Offer bonuses for “success”, the discovery of a safety-related bug. Import users who are cynical or careless to test the system. Spill some coffee on the keyboard. Hire college students part-time. Use outrageous inputs. Make the system wish it had never been built. Run the system 24 hours a day seven days a week for its life, not simply to confirm performance and functionality, but always stressing the system searching for the safety-related bug.

Vigorous configuration management practices must be enforced to track which versions of COTS products have been subjected to each test. Each time there is a version upgrade to a COTS product, the tests must be executed again.

Sound test strategies, including scripted and unscripted testing, that have a proven track record of identifying sources of errors within a system should continue to be used. Test strategies that have been successful at measuring the accuracy and precision with which software performs include:

- Black box testing: A testing strategy that derives test data solely form the requirements specification.
- White box testing: This is a complement of black box testing: a strategy that derives test data from knowledge of the program's internal structure.
- Gray box testing: This strategy derives test data by combining elements of black box and white box testing.

4.2 Management

There are management issues that are unique to COTS/NDI that are evaluated in the following section. The impact of these issues on safety certification was considered by the Subcommittee when recommendations were developed.

4.2.1 COTS/NDI Selection And Use Guidelines

Issue: A brief prepared by the "Open System Development" Subcommittee of the FAA Research, Engineering, and Development Advisory Committee in June, 1991, recommended that the FAA develop an acquisition strategy that would allow it to gain the greater capability, earlier and at less cost which can be achieved by using COTS, GOTS and NDI products. This recommendation is consistent with the widely accepted industry trend toward use of COTS/NDI components in system architectures, and with FAA Order 1810.6 which addresses NDI. There is, however, limited guideline for FAA system architects and developers to use in the selection of COTS/NDI products or on how to manage the use of the products throughout the life cycle of the system, to include operation and maintenance.

In many cases the FAA will represent a small percentage of the users of particular COTS/NDI products. And vendors are driven to fix errors and incorporate new features by the demands of the largest number of users of the product. The dilemma for the FAA is how to influence commercial vendors to satisfy their needs for products when they represent smaller market to the vendor.

Mitigation: The FAA should provide improved guidelines for the selection, engineering, and use of COTS/NDI in safety-critical systems. The guidelines must be compliant with the Federal Acquisition Regulation (FAR) and the Competition and Contracting Act. An inter-agency “consortium” should be considered to develop a common set of guidelines so vendors who want their products to be considered for use in Government computing systems clearly understand the requirements. Additionally, the “consortium” would collectively represent a larger market share and gain market influence.

Other organizations that are addressing this need include:

- NASA reportedly is in the process of developing a checklist of COTS/NDI selection criteria.
- The U.S. Air Force Joint Command Commercial-Off-The-Shelf (COTS) Supportability Working Group (CSWG) has developed guidelines
- ISO guidelines, being written by John Harauz of Ontario Hydro Nuclear, addresses qualification of COTS for different criticality levels for safety-critical and safety related applications.

The guidelines for selection and use of COTS/NDI in safety-critical systems could follow the model being prepared by ISO or one presented in the U.S. Air Force *Guidelines for Successful Acquisition and Management of Software Intensive Systems,* that contains a COTS Product Identification and Evaluation Process. Additionally, if the FAA develops profiles of types of products that will commonly be used together in the DSSA architecture concept discussed in Section 4.2.2, the FAA could enhance their influence of commercial vendors. The concept of product profiles is not new; it is one that X/Open, a standards consortium, has worked to develop so that standards verification testing can be performed for profiles of products.

4.2.2 Lack Of Insight Into COTS

Issue: Whether the COTS component is a widely-used operating system, such as UNIX, for a specific hardware platform, a shrink-wrapped product commonly available in retail stores, or a product available via a vendors' WEB page, the buyer of the product has little or no insight into how the product was manufactured or into the internal structure of the software. When shrink-wrapped software packages are produced for home or office computer use, the buyer may not be concerned about the quality control processes the manufacturer employs. But interest peaks if the product is to be integrated into a safety-critical application.

When components are custom-coded, there are standards that are followed that include independent review of requirements for how the development of the software will be planned, managed, and monitored. When a safety-critical system is comprised of COTS components, the project management procedures and development practices of each vendor become important in the overall assessment of safety. This may not be possible when commercial COTS components are incorporated into the architecture of the system.

The assurance practices of the vendor may not be known, or they may be known to be lacking. Assurance activities are those that will locate problems (e.g., errors, faults) in the development process and products, and will provide evidence that the software complies with its specifications. These activities are performed from the beginning of the software life cycle, through development. Sometimes the components are not fully-tested by the vendor. The software quality assurance practices that specify the requirements and standards to assure quality in the product may not be known. And there may be no visibility into how, or if, the component was verified as fulfilling the requirements.

Mitigation: The FAA, in collaborative arrangement with other Government organizations, should develop a process to certify levels of vendors compliance to software development best practices. The Software Capability Evaluation (SCE) based on the Software Engineering Institute (SEI) Capability Maturity Model (CMM), or the evolving ISO Software Process Improvement and Capability dEtermination (SPICE) should be considered as a mechanism to define and determine best practices. If components from a vendor that does not meet the strongest certification level of best practice compliance are used in a safety-critical architecture, the system integrator should be responsible for additional assurance requirements, such as architectural error containment techniques.

The FAA should encourage vendors to provide access to issue tracking reports of products that are being consider for an acquisition. It may be possible in the future to regulations that require COTS vendors to publish such information publicly.

4.2.3 COTS/NDI Capabilities And Limitations May Not Be Understood

Issue: Vendor product demonstrations are too frequently used as the primary basis of product selection. The performance and function of the product are not always as advertised resulting in poor assessment of the predicted success or failure of a product.

Mitigation: Buyers of COTS/NDI products should insist upon more control of initial product demonstrations through providing scenarios, platform or specific integrated product configurations to be demonstrated. Documentation and training should be made available for review before purchase of the product. Among other actions, the FAA should consider implementing a Beta test site laboratory for COTS products to ensure understanding of the product capabilities and limitations before the product is integrated into safety-critical systems. It is essential to identify problems with COTS early in the product life cycle, report them to the vendor, and encourage quick resolution.

4.2.4 Vendor/Supplier Dependency

Issue: Systems developed with components that are uniquely manufactured by one vendor or that run in limited environments risk obsolescence. The FAA is at the mercy of the vendor to produce and maintain the component.

Mitigation: COTS/NDI selection criteria should address multi-source, open system and open architecture products and warn about choosing products with proprietary interfaces. An open system solution provides for future growth of the system because enhanced components developed to interface standards can be “plugged” into the system. Conformance to standards improves the portability, extensibility and maintainability of the system. Unique products, for which second sources do not yet exist, should include additional safeguards, such as escrow of source code or other life-cycle safeguards.

4.2.5 Supportability

Issue: A major change for organizations accustomed to acquiring custom-developed products is the support life cycle of COTS/NDI products. The useful life of a vendor product may compare well with custom-developed products but the market driven nature of vendor support may well mean bug fixes may not be continued for more than a year or two. In general, bug fixes for the original version of the product are rolled forward into the next version of the product and all vendor support moves forward to this next version.

The nature of support varies greatly from vendor to vendor. Some will provide a help desk and bug fixes to the current version free or at a nominal cost. Others charge consultant fees or require paid subscription for the same services. In some cases the vendor support of a COTS component may be provided by second or third-tier suppliers, sometimes small “mom and pop” operations.

Changes to COTS products are market-driven and if the problem a component is experiencing does not effect the targeted user community, it may never be remedied. If a significant percentage of the user community indicate a desire for an enhancement it may be packaged in a new version or upgrade. Some vendors offer upgrades to new versions at a reduced cost to existing users while others require full payment.

Scheduling release updates to systems with multiple vendor products can be difficult because COTS/NDI product releases may be out of sync with the system release schedule. If a vendor does not ship on schedule or does not include an expected enhancement in a release, costly delays may incur. This can wreak havoc on development schedules, system functionality and long-term maintenance.

New features contained in version updates are sometimes difficult to integrate into an existing system. This presents not only technical challenges, but can impact the over-all schedule for system releases.

Mitigation: Clear guidance should be available for contract and program management personnel to insure these issues are appropriately addressed. This guidance should give explicit direction on how to assess the viability of the supplier during the product selection process. And the "market leverage" of the system should be considered when selecting a product.

A review of the vendor's commitment to scheduled releases should be conducted during the product evaluation process. Adherence to schedule is important because delays in release of one product may result in supportability issues of an associated component. A scheduled system release, for example, may include upgrade to a component that would be obsolete if not replaced by a certain date. This could result in complications because a vendor will not support out-of-date versions of an COTS/NDI component. Multi-vendor support must be closely coordinated

The acceptance criteria for version upgrades should be stated in the purchase contract to insure that proper documentation is available to facilitate integration, operation, and maintenance of the COTS/NDI component. When accepting a product, there should be a list of approved features that can be used to make sure designers don’t use “undocumented” features that may disappear in future releases.

If the life expectancy of the system exceeds the vendor support life cycle and modifications to the life expectancy are not possible, or if there are concerns that a software vendor may go out of business, then it is prudent to make provisions for a third party to maintain copies of the source code. It is also possible to contract the vender to provide continuing support for a product. Contractual provisions must be made that allow the Government or the prime contractor to assume responsibility for the maintenance of or enhancements to that code.

4.2.6 Life Cycle Costs

Issue: When developing any system the life expectancy of the system and life cycle costs must be considered. But there are additional factors, such as licensing and maintenance agreements, that must be considered when establishing the life cycle cost of systems comprised of COTS components. The full life cycle costs associated with COTS components are frequently underestimated because there are no standards for product licenses and maintenance agreements. For example, the number of “seats” or users that a license supports varies among vendors, or the license may be for one product that resides on a server but is available to multiple client workstations, or it may be explicitly for the server. One product may require software to be installed on each workstation with a site license, while another product requires licenses for each workstation. The maintenance agreements may provide on-site service within a specified amount of time, or only help-desk support. There are many variables to consider and it becomes increasing difficult to understand the various terms of agreements when there are numerous products.

There remain unresolved questions concerning liability in safety-critical system applications. For example, who is responsible when software failure results in a serious, major or catastrophic event? This question becomes more complex in a system with multi-vendor COTS components or multi-level product integrators and resellers.

Mitigation: The supportability and life cycle maintenance costs of the system must include vendor licensing, service agreements, and an assessment of the impact of cost to the system due to vendor instability or potential schedule delays for upgrades to COTS components. A performance assessment of the system may reveal that the COTS components require larger or faster hardware components to meet performance requirements.

As there is no standardization for support contracts and licensing agreements, careful consideration must be given to the contract language or the requirements specification, which specifies the vendors support responsibilities. Long-term warehousing of spares or provisions for long-term defect support can be expensive. The life expectancy of COTS/NDI component, and possible replacement products, should be evaluated within the context of the system life expectancy. Questions about configuration management, licensing by site vs. workstation, availability of site support and who provides the support, the product maintenance procedures, and the product distribution process should be addressed during the product selection process.

Throughout the COTS life cycle, books and training are often available at a lower cost through the vendor or commercial sources because there is a broad demand for it and development costs are spread over a large user base. Increasingly, software is distributed via WEB servers over the internet to reduce cost.

Clear understanding of ownership and responsibility during acceptance and maintenance of each product is essential before a contractual agreement is made to purchase a COTS product or use a NDI component. Clear understanding of fiscal responsibilities between the COTS vendor, the NDI reuse library custodian, the system integrator, and the system buyer must be documented. In some cases, there may be concern that the vendor may not be solvent and the software source code may be placed in “escrow” to protect the viability of the system.

COTS vendors will need to be informed of the intended use of their product in a safety-critical system and they may need to consider acquiring liability insurance. The vendor or the system developer may be able to purchase the insurance through Specialty Risk Pools for extensive costs. The integration of COTS products into safety-critical systems must involve vendor compromises. Perhaps new laws are necessary to protect the vendor from the exploitation of such compromises. The legal implications of using COTS needs to be investigated in depth, soon.

4.2.7 Reuse Libraries

Issue: The domain engineering scenario described in Section 1.3 and the architectural approach identified in Section 4.2.2 rely on domain-specific reusable NDI artifacts. The reuse library will contain everything the software organization needs to know in order to create, modify, maintain, and evolve a system. These reusable NDI artifacts will include code, process models, requirements, and documentation, all of which will conform to standard definitions for data, process, and delivery system components to enable them to be assembled to form complete applications.

These software artifacts may be developed by system integrators or obtained from reuse libraries such as the DoD Software Technology for Adaptable, Reliable Systems (STARS) Asset Source for Software Engineering Technology (ASSET), the NASA Multi-media, Oriented Repository Environment (MORE) libraries, or commercial libraries such as Object Windows Library from Borland International Inc.

Many of the supportability and life cycle cost issues identified previously are applicable to NDI components. Use of components from reuse libraries present unique certification, library management, life cycle maintenance, and distribution issues.

Mitigation: The FAA should begin now to plan for a reuse library with domain-specific software artifacts, i.e., navigation, weather, automation, surveillance, and other reusable software. The FAA should explore the possibilities of utilizing components available from existing reuse libraries, such as ASSET and MORE. Additionally, guidelines for test, certification, library management, life cycle maintenance, customization, and distribution should be developed.

Clear guidelines for life cycle support and distribution of cost among users should be developed. Roles and responsibilities must be explicitly identified, and procedures for development of potential NDI components, change requests, maintenance, release schedules, documentation, interface standards, and distribution should be developed.

4.2.8 People

Issue: Building any software-intensive system is hard, building a safe one even harder. The problem of building a safe system is made worse by increasing system complexity, driven by new, demanding requirements. (Free flight is such a requirement.) The experience and quality of the senior management and technical talent is perhaps the single most important factor in achieving success. The “outstanding people” problem has been exacerbated by the economy and the environment. If the trend continues, it will become increasingly difficult for companies building safety-critical systems for the government to recruit and keep outstanding software managers, architects, and developers in competition with the commercial software product developers.

Mitigation: By using COTS, a project can reduce the number of people required, easing the management load and reducing the number of needed outstanding people. Assuming the COTS does not introduce new safety concerns, the increase in the ratio of outstanding to average performers should improve quality and, hence, safety. Furthermore, it should be easier to recruit good people if they are working with mainstream commercial products.

5. Recommendations

Based on the technical analysis in the preceding sections and the overall goal to assess the adequacy of current safety certification processes, the Subcommittee makes the following recommendations:

5.1 In-depth Analysis of Current Practices

The introduction of COTS/NDI components and resultant issues identified in Section 4 lead the Subcommittee to conclude that changes to current processes are necessary and that the FAA should fund an in-depth analysis of the current safety engineering and certification processes. Careful analysis should be done to determine what changes in current processes, and organizational roles and responsibilities are required to mitigate risks introduced by this emerging technology. FAA systems will continue to grow in the size and complexity of the tasks they must perform. The ultimate goal is to increase the ability of engineers and managers to understand and deal effectively with systems whose real complexity appears to be far beyond their capacity to assess adequately given current tools and techniques.

The proposed in-depth analysis would address the following areas:

- Develop COTS/NDI selection and engineering use guidelines, to include identification, classification, and reuse of architectural templates. The guidelines should address roles and responsibilities, and engineering tasks to be performed in the context of the system life cycle.
- Investigate new ideas for measuring and estimating the complexity of systems. Identify specific metrics that can be used to judge the quality of safety based on the complexity of the system.
- Develop a tailored life cycle model that addresses COTS/NDI components used in safety-critical systems. A goal should be to ensure the life cycle takes advantage of COTS/NDI components to reduce the cost and time required to develop high-assurance, distributed systems.
- Develop a process to conduct preliminary risk assessments of systems that plan to use COTS/NDI components. Issues rules to programs/integrators that plan to use COTS/NDI components.

- Identify new methods to test and validate safety-critical systems which are not dependent on source code analysis.
- Investigate ways to reduce the cost and time required to establish high confidence in a system. The ultimate goal is to achieve a level of confidence comparable to having exhaustively tested or proven the behavior of every part of the system. The promise of rapid development of systems comprised of commercial products requires acceleration of assurance processes.
- Investigate ways to reduce the cost and time required to reestablish high confidence in an evolving system after a change is made. It should be possible to bound the propagation of effects from an upgrade of a COTS/NDI component.
- Investigate ways to deal with the interdependent, safety-critical and mission-critical properties of fault tolerance, performance, functional correctness, security, human-machine interaction, and other issues.
- Explore domain specific architecture techniques that would facilitate development and certification of air traffic control, avionics, surveillance, weather, and navigation systems.
- Investigate new ideas for use of COTS/NDI components within domain specific architectures that would "fire wall" functionality. Develop defensive design techniques to mitigate COTS/NDI anomalies.
- Develop guidelines for use of NDI components acquired from domain-specific and general purpose reuse libraries. Among other things, these guidelines should address test and certification processes, database access and maintenance procedures, and product distribution procedures to include acquisition of components available via the internet.
- Demonstrate the cost-effectiveness of these techniques in typical FAA applications and establish technology transfer mechanisms to bring them into the FAA mainstream.

Analysis of organizational roles and responsibilities should include:

- Investigate ways to involve the verification and validation, safety engineering, and quality assurance personnel earlier in the system specification phase.
- Assess modification of the certification process to employ a quick analysis methodology early in the system life cycle to address the acceptability of the solution of the system under consideration.
- Identify ways to effectively communicate to assurance and certification organizations the impact of frequent upgrades of COTS/NDI components and prepare for on-going and overlapping certification activities. Ensure they understand the risks associated with not upgrading a product that may become insupportable by the vendor.
- Become a Beta test site for COTS products that are candidates for use within FAA domain specific architectures.
- Promote software technology and process improvement techniques based on established best practice techniques.
- Explore ways to expand current tracking of anomalies of COTS products by keeping statistics on product use throughout the computing industry.

5.2 Inter-Agency Initiative

The Subcommittee recommends the FAA host an inter-agency initiative to promote a consolidated approach to integration of COTS/NDI in safety-critical systems. The implication of the issues addressed in this report are of interest to other Government organizations that have safety-critical systems. The Subcommittee proposes that the FAA consider a collaborative agreement with other Government organizations that are facing these same challenges. The advantage of a collaborative effort among affected Government organizations will be development of standard guidelines and processes for COTS vendors, system integrators, and for procuring Government organizations. In addition, it will promote the exchange of information on COTS, and broaden market influence.

Collectively, the Government organizations increase their influence due to expanded market share and can consolidate requirements they levy on vendors and integrators. Vendors that chose to have their products considered for the safety-critical environment will have a clear understanding of expectations. Additionally, the following long-range goals may be achievable through this collaborative effort:

- Vendors will be encouraged to provide configuration files that allow tailoring of their products by masking out unused functionality. It is envisioned that this initially will occur at the HCI level, but eventually it is likely to occur at the functional level. Government might consider accelerating this process by incentivizing COTS vendors.
- Vendor processes and component quality levels will be assessed and rated by independent organizations (not necessarily Government). Rather than an ISO 9000 standard, there might be very specific test, reliability, and process questions that are assessed and used by system integrators during COTS product selection. This information would also be used by verifiers and certifiers to determine appropriate levels of testing and areas of focus.
- The current problem of rapidly evolving standards is likely to be balanced in the future by the fact that standards are the only apparent way to ensure “similar usage” and achieve the universally desired high reliability of complex systems. Once it becomes clear how dependent we are on these standards to achieve this reliability at a systems level, the current volatility of standards will become more constrained. This doesn’t imply less technological change--it simply implies that certain characteristics of future changes are likely to be more tightly controlled so that we can retain the global benefits shared by all.

Appendix A References

Note: To produce a comprehensive bibliography of the material reviewed for preparation of this report would be an enormous undertaking. The references presented here are intended only to provide interested readers with a few points of entry into the literature.

- Defense Science Board Task Force Report, *Acquiring Defense Software Commercially*, 1994
- Software Productivity Consortium Second Annual Executive Round Table, "*Putting COTS Software to Work*" Proceedings, October 19-20, 1994
- TRW Conference Proceedings, *Issues in COTS Integration*, 1994
- Leveson, Nancy G. (1995*) Safeware: System Safety and Computers*, Addison-Wesley
- Neumann, Peter G. (1992*) Computer-Related Risks*, ACM Press.
- Peterson, Ivars (1995) *Fatal Defect: Chasing Killer Computer Bugs*, Time Books
- Landauer, Thomas K. (1995*) The Trouble with Computers: Usefulness, Usability, and Productivity*, Massachusetts Institute of Technology
- Roland, H.E. and Moriarty, Brian (1990) *System Safety Engineering and Management*, John Wiley & Son
- Hammer, Willie (1972) *Handbook of System and Product Safety*, Englewood Cliffs, NJ: Prentice-Hall
- Stephans, Richard A., Talso, Warner W., (1993) *System Safety Analysis Handbook*, VA: System Safety Society
- *Commercial System Safety Program Requirements*, SS-STD-882, System Safety Society (1995)
- Software Engineering Institute, Draft *Software Acquisition Capability Maturity Model, 1995*

- *Software Engineering Institute, Key Practices of the Capability Maturity Model*, Version 1.1, February 1993
- Proceedings of the SEI/MCC Symposium on the Use of COTS in Systems Integration, March 17, 1995
- Neumann, Peter G., (1986) On Hierarchical Design of Computer Systems for Critical Applications, IEEE Transactions on Software Engineering, Vol. SE-12, No 9

Government Documentation

- FAA-STD-026, NAS Software Development: Levies 2167A Requirement Tailoring Guide for FAA-STD-026
- MIL-STD-498, Software Development and Documentation
- MIL-STD-882C, System Safety Program Requirements
- FAA Order 1810.1F, Acquisition Policy
- FAA Order 1810.6, Policy for Use of NDIs in FAA Acquisition
- RTCA / DO-178B, Software Considerations in Airborne Systems and Equipment Certification
- FAA Program Manager's Guide, April 1994
- ASU-120 Briefing: "Acquisition in the FAA- A New Approach"
- FAR 23.1309, General Aviation Airplanes
- FAR 27.1309, Rotorcraft
- Department of the Air Force, Guidelines for Successful Acquisition and Management of Software Intensive Systems, Version 1.1, February 1995

Appendix B Acknowledgments

This work represents the collective effort of numerous individuals from TRW's System Integration Group (SIG). Without the contributions of technologists from this diverse skill set, a document of this breadth could not have been developed. Significant contributions were submitted by Ken Zemrowski, R.J. Langley, and Amir Abouelnaga. The principal investigators and authors are identified below.

Gail Cochrane
Manager, Process Coordination
TRW's Systems Integration Group
One Federal Systems Park Drive
Fairfax, VA 22033-4411
Phone: (703) 803-4747
e-mail: gail.b.cochrane@trw.com

Al Babbitt, Ph.D.
Senior Technical Advisor to the Vice President and General Manager
TRW's Systems Integration Group
One Federal Systems Park Drive
Fairfax, VA 22033-4411
Phone: (703) 803-5000
e-mail: babbitta@gisdbbs.fp. trw.com

Acknowlegmemts

Acknowledgment for the significant contributions by the following individuals:

Principal Contributors:

Mr. Bruce Landsberg
Executive Director
AOPA Air Safety Foundation
421 Aviation Way
Frederick, MD 21701

Mr. John F. Zugschwert
Vice President
Government Marketing
TEXTRON
1101 Pennsylvania Avenue NW
Suite 400
Washington, DC 20004

Contributors:

George R. Allen, Ph.D.
Senior Software Engineer
TRW
Fairfax, VA 22033
COTS In Safety Critical Systems

Dr. William W. Agressti
The Mitre Corporation
7525 Cosdhire Drive
McLean, VA 22102
Balancing User Satisfaction Project Resources and Selected COTS Products

Mr. Amir Abouelnaga
Senior Engineer
TRW's Sustems Integration Group
One Federal Systems Park Drive
Fairfax, VA 22033-4411
Contributor: COTS In Safety Critical Systems

Satya N. Atluri, Ph.D.
Institute Professor
Georgia Institute of Technology
Computational Modeling Center
Atlanta, GA 30332-0356

Al Babbitt, Ph.D.
Senior Technical Advisor to the Vice President and General Manager
TRW's Sustems Integration Group
One Federal Systems Park Drive
Fairfax, VA 22033-4411
Contributor: COTS In Safety Critical Systems

Mr. Richard Ballard
RLB Associates
Fairfax, VA
Certification Processes For Advanced Confirguration of Aircraft

Mr. Arnold R. Beckhardt
Software Engineering Technology Inc.
2270 Indian Riaver Blvd.
Vero Beach, FL 32960
Classroom Software Engineering

Gerard T. Capraro, Ph.D.
Capraro Technologies \
311 Turner Street, Suite 410
Utica, NY 13501
Views Of The Situation & Some Technology Areas That May Help
The FAA

Mr. David N. Card
Software Productivity Solutions, Inc.
122 4th Avenue

Indialantic, FL 32903
Streamline Integrated Metrics Approach

Mr. Frank J. Colson
Executive Director
DoD Policy Board on Federal Aviation
SAF/AQRT 1060 Air Force Pentagon
Washington, DC 20330-1060
Decision Process Between Competing Technologies

Ms. Gail Cochrane
Manager, Process Coordination
TRW's Sustems Integration Group
One Federal Systems Park Drive
Fairfax, VA 22033-4411
Contributor: COTS In Safety Critical Systems

The Honorable Susan M. Coughlin
Senior Vice President and General Manager
Transportation Systems
BDM Federal, Inc.
1501 BDM Way, Room 3B312
McLean, VA 22102
Human Performance & Safety; COTS Product Validation D

Mr. Joe Dean
Tecolote Research, Inc.
Bedford, MA
Practical Software Management; A Joint Logistic Commander's Report

Dr. George H. Dinsmore
SoHaR, Inc.
8421 Wilshire Blvd.
Beverly Hills, CA 90211
Electronic Commerce/Electronic Data Interchange, Analysis of Human Performance Records. National Software Data and Information Repository

Mr. Larry E. Druffel
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213
Software Unintended Functions; Human Factors Integration

Mr. Peter B. Dyson
Software Productivity Solutions
122 4th Avenue
Indialantic, FL 32903
Certification of Reusable Software Components

VADM Donald D. Engen,USN(ret)
809 Duke Street
Alexandria, VA 22314
Educational And International Implications; A Fresh Look Sought

Mr. Ralph Eschenbach
Vice President of New Business Development
Trimble Navigation, Ltd.
645 N. Mary Avenue
Sunnyvale, CA 94086

Mr. John E. Gaffney, Jr.
Software Productivity Consortium
SPC Bldg., 2214 Rock Hill Road
Herndon, VA 22070
Measurement Driven Management, Fault Tolerance Analysis

Mr. Charles Huettner
NASA/FAA
Washington, DC
High Performance Computing And Communications,
Accomplishments & Plans

Mr. Watts S. Humphrey
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213
Assistance Offer

Mr. R.J. Langley
Chief Engineer for Automatic Identification Systems
TRW's Sustems Integration Group
One Federal Systems Park Drive
Fairfax, VA 22033-4411
Contributor: COTS In Safety Critical Systems

Mr. Ted W. Keller
IBM Federal Services Company

Mr. Joseph L. McCormick
200 Deerfox Lane
Lutherville, MD 21093
Technologies That Will Make An ATC System Difference

Dennis K McLaughlin, Ph.D.
Head, Department of Aerospace Engineering
The Pennsylvania State University
233 Hammond Building
University Park, PA 16802

The Honorable John L. McLucas
1213 Villamay Boulevard
Alexandria, VA 22307
People Qualifications And Training To Meet Future Challenges In FAA Technology

Mr. Francis D. McVey
McDonnell Douglas Aerospace
P.O. Box 516
St. Louis, MO 63166
Smart Composite Structures, Subsystem Intetgration, Avionics Architecture

Mr. Gerald E. Murine
Metriqs, Inc.
33961 Calle de Bonanza
San Juan Capistrano, CA 92675
Software Quality Management (RLSQF), Optismism Resource Allocator, the ORA and Human Factor Analysis

Mr. Don O'Neill

Software Engineering Consultant
9305 Kove Way
Gaithersburg, MD 20879
Software Issues; Standard of Excellence Checklist For Plans, Requirements, Specifications, Design & Code, Test Procedure

Mr. Lawrence H. Putnam
Quantitative Software Mgmt., Inc.
2000 Corporate Ridge, Suite 900
McLean, VA 22102
Strategic Issues In Managing Software Cost And Control

Mr. Joe Raynus
InfoDynamics, Inc.
15 Pelham Road
Lexington, MA 02173
Safety Risks of Software Unreliability, Etc.

Mr. Norman F. Schneidewind
Naval Postgraduate School
Monterey, CA 93943
Software Reliability; Space Shuttle, Failure Data, Validatory Metrics, Applying Metrics To Multiple Projects; Predicting Quality of Space Shuttle Software

Mr. Bill Schultz
Vice President
Engineering & Maintenance
General Av_ation Manufacturers Association

Edwin B. Stear, Ph.D.
Corporate Vice President for Technology Assessment
The Boeing Co.

Mr. Robert C. Tausworthe
Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive
Pasadena, CA
Information Technology Outlook, a JPL Report August ‘95

C. E. Velez, Ph.D

Chairman and Chief Executive Officer
CTA Incorporated
6116 Executive Boulevard, Suite 800
Rockville, MD 20852
Requirements For Organizational Change - The Human Side Of
Regulation And Certification Reform

Robert E. Whitehead, Ph D.
Acting Associate Administrator
Office of Aeronautics (Code R)
National Aeronautics and Space Administration
300 E Street, SW
Washington, DC 20546
Fly By Light / Power By Wire Changes In The Aircraft Effect
Management Control

Earl L Wiener. Ph.D.
University of Miami
Department of Management Science
School of Business Administration
417 Jenkins
Coral Gables, FL 33124
Human Vigilance And Monitoring; Management of Human Error

Mr. Fred E. Wood
Jet Propulsion Laboratory
Pasadena, CA

Dr. Andres G. Zellweger
Director
Office of Aviation Research
Federal Aviation Administration
800 Independence Avenue, SW
Washington, DC 20591
Referral To NASA / FAA Contact / Collaboration

Mr. Ken Zemrowski
Senior Engineer
TRW's Sustems Integration Group
One Federal Systems Park Drive
Fairfax, VA 22033-4411

Contributor: COTS In Safety Critical Systems

Mr. Stuart H. Zueben
The Ohio State University
Columbus, Ohio
Systems Engineering Training; How Academia Can Help

Committee Sponsor:
Dr. Andres Zellweger
Director
Office of Aviation Research
Federal Aviation Administration
800 Independence Avenue, SW
Washington, DC 20591

Special Assistant:
Ms. Lee Olson, AAR-200
Federal Aviation Administration
800 Independence Avenue, SW
Washington, DC 20591

Special thanks to the RE&D Committee Members for their contributions.

Members:
Lt Gen James A. Abrahamson. USAF (Ret)
International Air Safety Corporation
700 13th Street, NW
Suite 1160
Washington, DC 20005

Captain Patricia W. Andrews
Chief Pilot
Mobil Corporation
Aircraft Services Department
P. O. Box 16980
Dulles International Airport
Washington, DC 20041-6980

Satya N. Atluri, Ph.D.
Institute Professor
Georgia Institute of Technology

Computational Modeling Center
Atlanta, GA 30332-0356

Captain Robert G. Buley
Manager, Flight Operations Development
Northwest Airlines (Department N-7400)
5101 Northwest Drive
St. Paul, MN 55111

Mr. Frank J. Colson
Executive Director
DoD Policy Board on Federal Aviation
SAF/AQKT 1060 Air Force Pentagon
Washington, DC 20330-1060

The Honorable Susan M. Coughlin
Senior Vice President and General Manager
Transportation Systems
BDM Federal, Inc.
1501 BDM Way, Room 3B312
McLean, VA 22102

VADM Donald D. Engen,USN(ret)
809 Duke Street
Alexandria, VA 22314

Mr. Ralph Eschenbach
Vice President of New Business Development
Trimble Navigation, Ltd.
645 N. Mary Avenue
Sunnyvale, CA 94086
Delores M. Etter, Ph.D.
Electrical & Computer Engineering Department
Campus Box 425
University of Colorado
Boulder, CO 80309-0425

The Honorable Najeeb E. Halaby
Drawer Y
175 Chain Bridge Road
McLean, VA 22101

Wesley L. Harris, Ph.D
Associate Administrator
Office of Aeronautics (Code R)
National Aeronautics And Space Administration
300 E Street, S.W.
Washington, DC 20546

Mr. George P. Howard
President
Airports Council International - North America
1775 K Street, NW
Suite 500
Washington, DC 20006

Ms. Margaret T. Jenny
Acting Technical Director
System Analysis Division, CAASD
The MITRE Corporation
Mail Stop W395
7525 Colshire Drive
McLean, Virginia 22102

Mr. Bruce Landsberg
Executive Director
AOPA Air Safety Foundation
421 Aviation Way
Frederick, MD 21701

John K Lauber, Ph.D.
Vice President
Corporate Safety and Compliance
Delta Airlines (Department 025)
Hartsfleld-Atlanta International Airport
Atlanta, GA 30320

Ms. Mary Rose Loney
Director of Aviation
Philadelphia International Airport
Terminal E Departures, 2nd Floor
Philadelphia, PA 19153

General James McDivitt, USAF (ret.)

9146 Cherry Avenue
Box 224RR1
Rapid City, Ml 49676
Dennis K. McLaughlin, Ph.D.
Head, Department of Aerospace Engineering
The Pennsylvania State University
233 Hammond Building
University Park, PA 16802

The Honorable John L. McLucas
1213 Villamay Boulevard
Alexandria, VA 22307

Mr. Joseph L. McCormick
Aerospace Consultant
200 Deerfox Lane
Lutherville, MD 21093

Mr. John W. Olcott
President
National Business Aircraft Association, Inc.
1200 Eighteenth Street, NW
Washington, DC 20036

Mrs. Nancy Price
Special Assistant
Hughes Canada Systems Division
13951 Bridgeport Road
Richmond, British Columbia V6V1J6

Jack E. Snell, Ph.D.
Deputy Director
Building and Fire Research Laboratory
National Institute of Standards &Technology
Building 226, Room B-216
Gaithersburg, MD 20899

Mr. John P. Stenbit
Vice President and General Manager
TRW Systems Integration Group (FP1/7190)
One Federal Systems Park Drive
Fairfax, VA 22033

C. E. Velez, Ph.D
Chairman and Chief Executive Officer
CTA Incorporated
6116 Executive Boulevard, Suite 800
Rockville, MD 20852

Mr. Dale S. Warren
889 Long Hollow Circle
Durango, CO 81301-7090

Robert E. Whitehead, Ph D.
Acting Associate Administrator
Office of Aeronautics (Code R)
National Aeronautics and Space Administration
300 E Street, SW
Washington, DC 20546

Earl L Wiener. Ph.D.
University of Miami
Department of Management Science
School of Business Administration
417 Jenkins
Coral Gables, FL 33124

Mr. Christopher Witkowski
Director of Air Safety & Health
Association of Flight Attendants
1625 Massachusetts Avenue, NW
Washington, DC 20036

Mr. John F. Zugschwert
Vice President
Government Marketing
TEXTRON
1101 Pennsylvania Avenue NW, Suite 400
Washington, DC 20004